ISC.CISSP-CN.v2026-10-05.q802

Exam Code:	CISSP-CN
Exam Name:	Certified Information Systems Security Professional (CISSP中文版)
Certification Provider:	ISC
Free Question Number:	802
Version:	v2026-10-05
# of views:	318
# of Questions views:	8020
https://www.freepdfdumps.com/ISC.CISSP-CN.v2026-10-05.q802.html	

NEW QUESTION: 1
在採購新資訊系統的過程中，發現系統規格中未涵蓋部分安全要求。下列哪一項最可能是造成這種情況的原因？
A. 採購員缺乏技術知識。
B. 採購過程中安全要求發生了變化。
C. 供應商的投標團隊中沒有安全專業人員。
D. 安全需求描述不足。
Answer: D (LEAVE A REPLY)
The most likely reason for some of the security requirements not being addressed in the system specification during the procurement of a new information system is that the description of the security requirements was insufficient. The description of the security requirements is the part of the procurement document that specifies the security objectives, criteria, standards, and measures that the system must meet or comply with. If the description of the security requirements is insufficient, vague, ambiguous, incomplete, or inaccurate, then the system specification may not reflect or satisfy the security needs and expectations of the organization.
The procurement officer lacking technical knowledge, the security requirements changing during the procurement process, and there being no security professionals in the vendor's bidding team are not the most likely reasons for this problem, as they do not directly affect the quality or clarity of the description of the security requirements.

NEW QUESTION: 2
攻擊者是否能□無限期地登入並利用 Web 服務？
A. 警報管理
B. 密碼管理
C. 會話管理
D. 身分管理 (IM)
Answer: C (LEAVE A REPLY)

Session management is the process of controlling and maintaining the state and information of a user's interaction with a web service. It involves creating, maintaining, and terminating sessions, as well as ensuring their security and integrity. An attacker who is able to remain indefinitely logged into a web service is exploiting a weakness in session management, such as the lack of session expiration, session timeout, or session revocation. Alert management, password management, and identity management (IM) are all related to security, but they do not directly address the issue of session management.

NEW QUESTION: 3
下列何者最能描述執行安全認證的目的？
A. 辨識系統威脅、漏洞和可接受的風險水平
B. 正式確認是否符合安全策略與標準
C. 正式確認風險緩解和風險分析已完成
D. 驗證系統架構及其與其他系統的互連是否有效實現
Answer: B (LEAVE A REPLY)
The best description of the purpose of performing security certification is to formalize the confirmation of compliance to security policies and standards. Security certification is the process of evaluating and validating the security posture and compliance of a system or network against a set of predefined criteria, such as security policies, standards, regulations, or best practices.
Security certification results in a formal statement or document that attests the level of security and compliance achieved by the system or network.

NEW QUESTION: 4
一家透過 Tier 4 資料中心提供資訊技術 (IT) 服務的公司正在準備全公司範圍的業務連續性規劃 (BCP)。IT 經理應該注意下列哪些故障？
A. 應用程式
B. 存儲
C. 電源
D. 網絡
Answer: A (LEAVE A REPLY)
A company whose IT services are being delivered from a Tier 4 data center should be most concerned with application failures when preparing a companywide BCP. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include a risk assessment, a business impact analysis, a recovery strategy, and a testing and maintenance plan.
A Tier 4 data center is the highest level of data center classification, according to the Uptime Institute. A Tier 4 data center has the highest level of availability, reliability, and fault tolerance, as it has multiple and independent paths for power and cooling, and redundant and backup components for all systems. A Tier 4 data center has an uptime rating of 99.995%, which means it can only experience 0.4 hours of downtime per year. Therefore, the likelihood of a power, storage, or network failure in a Tier 4 data

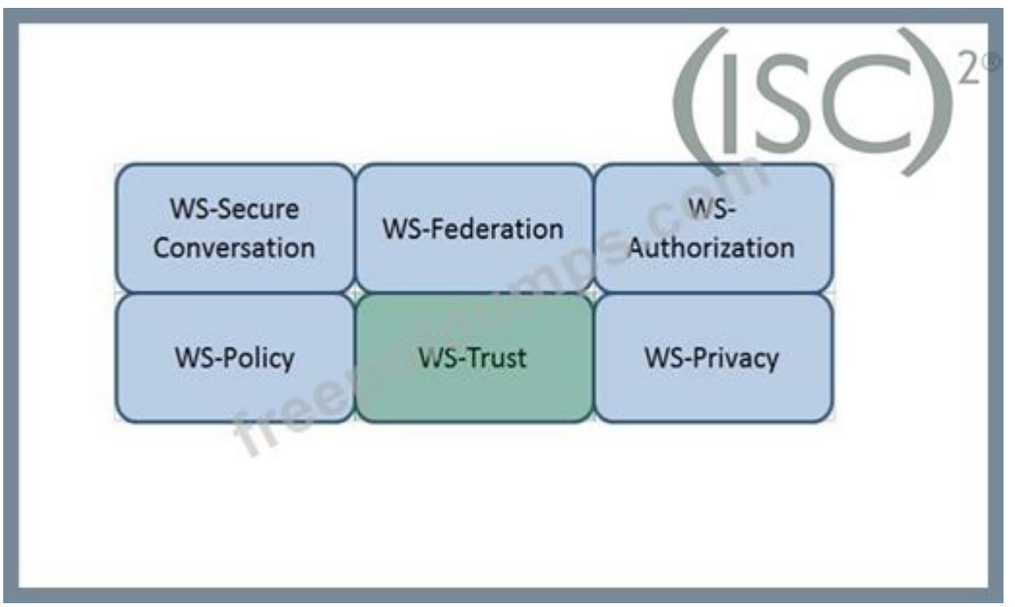
center is very low, and the impact of such a failure would be minimal, as the data center can quickly switch to alternative sources or routes.
However, a Tier 4 data center cannot prevent or mitigate application failures, which are caused by software bugs, configuration errors, or malicious attacks. Application failures can affect the functionality, performance, or security of the IT services, and cause data loss, corruption, or breach. Therefore, the IT manager should be most concerned with application failures when preparing a BCP, and ensure that the applications are properly designed, tested, updated, and monitored.

NEW QUESTION: 5
在軟體定義網路 (SDN) 中實施安全設計原則時應避免哪種依賴關係？
A. 混合
B. 圓形
C. 動態
D. 靜態
Answer: B (LEAVE A REPLY)
Circular dependencies occur when two or more components or entities depend on each other in a way that creates a circular chain of dependencies. This can lead to issues such as deadlock, where components wait for each other indefinitely, and it can make the system more difficult to manage and secure. To ensure the reliability and security of an SDN environment, it's important to minimize or eliminate circular dependencies among components.

NEW QUESTION: 6
開發團隊的安全訓練應在系統開發生命週期 (SDLC) 的哪個階段開始？
A. 開發/收購
B. 口動
C. 實施/評估
D. 處置
Answer: (SHOW ANSWER)
Security training for the development team should begin in the initiation phase of the System Development Life Cycle (SDLC). This is the phase where the security requirements and objectives are defined and the project scope and feasibility are determined. The development team should be aware of the security expectations and best practices from the start of the project, and receive continuous training throughout the SDLC. The other phases are not the best time to start security training, as they involve more specific tasks such as design, coding, testing, deployment, and maintenance.

NEW QUESTION: 7
熱點問題
哪個 Web 服務安全 (WS-Security) 規範規定了安全性令牌的核發、續訂和驗證方式？請點選下圖中的正確規範。

Answer:



NEW QUESTION: 8
在大容量網路上部署入侵偵測系統 (IDS) 時，需要在多個感測器之間分配負載會口生哪些技術問題？
A. 會話連續性
B. 代理身份驗證失敗
C. 感測器過載
D. 同步感測器更新
Answer: A (LEAVE A REPLY)
Session continuity is the ability to maintain a connection between a client and a server without interruption or loss of data. When deploying an IDS on a high-volume network, the need to distribute the load across multiple sensors would create a technical problem of session continuity, as the sensors may not be able to track the state of the sessions and correlate the packets from different sources. This could result in false positives or false negatives, or degrade the performance of the IDS.

NEW QUESTION: 9
哪種攻擊定義了插入軟體以觸發惡意功能的程式碼段？
A. 網路釣魚
B. 薩拉米香腸
C. 後門
D. 邏輯炸彈
Answer: (SHOW ANSWER)
A logic bomb is a piece of code that is inserted into software to trigger a malicious function when a certain condition is met, such as a specific date, time, or event. A logic bomb can cause various types of damage, such as deleting or encrypting data, crashing the system, or launching other attacks. A logic bomb is often hidden or disguised within legitimate software, making it difficult to detect or prevent. A logic bomb is different from phishing, salami, or back door attacks, which are defined as follows:
Phishing is a type of social engineering attack that uses fraudulent emails or websites to trick users into revealing their personal or financial information, or installing malware on their devices.
Salami is a type of fraud that involves stealing small amounts of money or data from multiple sources over time, hoping that the theft will go unnoticed or be ignored.
Back door is a type of covert access that bypasses the normal authentication or authorization mechanisms of a system or network, allowing unauthorized users or attackers to gain access or control.

NEW QUESTION: 10
下列哪一項是資料保留策略的主要目標？
A. 確保資料被正確銷毀。
B. 確保可以在 datA 上進行資料恢復。
C. 確保資料在預定時間口的完整性和可用性。
D. 確保資料在預定時間口的完整性和保密性。
Answer: (SHOW ANSWER)
A data retention policy is a document that specifies the rules and guidelines for how long and under what conditions an organization should retain its data. The main goal of a data retention policy is to ensure the integrity and confidentiality of data for a predetermined amount of time.
Integrity means that the data is accurate, complete, and consistent, and that it has not been modified or corrupted by unauthorized parties. Confidentiality means that the data is protected from unauthorized access or disclosure, and that it respects the privacy and security of the data owners or subjects. A data retention policy can help an organization to comply with the legal or regulatory requirements, to support the business or operational needs, and to reduce the storage or management costs of the data.
Ensuring that data is destroyed properly, ensuring that data recovery can be done on the data, and ensuring the availability of data for a predetermined amount of time are not the main goals of a data retention policy, as they are related to the disposal, restoration, or accessibility of the data, not the integrity or confidentiality of the data.

NEW QUESTION: 11
下列哪一項是線上憑證狀態協定 (OCSP) 最常見的用途？
A. 取得X.509數位憑證的到期日
B. 取得X.509數位憑證的吊銷狀態
C. 取得X.509數位憑證的作者姓名
D. 驗證 X.509 數位憑證的有效性
Answer: B (LEAVE A REPLY)
The most common use of the Online Certificate Status Protocol (OCSP) is to obtain the revocation status of an X.509 digital certificate. A digital certificate is a document that binds the identity and public key of an entity, such as a person, a device, or a website, and is issued and signed by a trusted authority, such as a certificate authority (CA). A digital certificate can be used for various purposes, such as authentication, encryption, or digital signature. A digital certificate can also be revoked by the CA for various reasons, such as expiration, compromise, or misuse.
OCSP is a protocol that allows a client, such as a web browser, to query the CA or a designated responder about the current status of a digital certificate, such as valid, revoked, or unknown.
OCSP can provide a faster and more efficient way of checking the revocation status of a digital certificate, compared to other methods, such as certificate revocation lists (CRLs) or delta CRLs.

NEW QUESTION: 12
下列哪項災難復原 (DR) 測試流程最不可能幹擾正常的業務運作？
A. 平行
B. 模擬
C. 桌面式
D. 切換
Answer: C (LEAVE A REPLY)
A table-top DR testing process is the least likely to disrupt normal business operations, as it involves only a discussion or a walkthrough of the DR plan with the key stakeholders and participants. No actual systems or resources are involved in the test, and no disruption or downtime is expected. A parallel DR testing process involves activating the backup site and running the systems in parallel with the primary site, which may cause some performance issues or conflicts. A simulation DR testing process involves simulating a disaster scenario and testing the response capabilities of the staff and the systems, which may cause some stress or confusion. A cut-over DR testing process involves switching the operations entirely to the backup site and shutting down the primary site, which may cause the most disruption and risk of the DR testing processes.

NEW QUESTION: 13
安全架構師被指派負責確保組織電子記錄的完整性。下列哪一種方法提供了最強的完整性？
A. 時間戳
B. 加密
C. 雜湊

D. 數位簽名

Answer: D (LEAVE A REPLY)

The method that provides the strongest level of integrity for the organization's electronic records is the digital signature. A digital signature is a cryptographic technique that uses public key cryptography and hashing to verify the authenticity, integrity, and non-repudiation of an electronic record. A digital signature is created by applying a hash function to the electronic record, which produces a unique and fixed-length value called a message digest. The message digest is then encrypted with the sender's private key, which produces the digital signature. The digital signature is attached to the electronic record and sent to the receiver. The receiver can verify the digital signature by decrypting it with the sender's public key, which produces the message digest. The receiver can then apply the same hash function to the electronic record, which produces another message digest. The receiver can then compare the two message digests, and if they match, it means that the electronic record is authentic, intact, and originated from the sender. A digital signature provides the strongest level of integrity for the electronic record, as it ensures that the electronic record has not been altered, tampered, or corrupted during transmission or storage, and that the electronic record can be traced back to the sender. A digital signature also provides other security benefits, such as confidentiality, authentication, and non-repudiation. Time stamping, encryption, and hashing are not methods that provide the strongest level of integrity for the organization's electronic records. Time stamping is a technique that records the date and time of an event, such as the creation, modification, or transmission of an electronic record. Time stamping can help to establish the chronology, validity, or expiration of an electronic record, but it does not ensure the integrity of the electronic record. Encryption is a technique that transforms the data of an electronic record into an unreadable form, using a secret key or algorithm. Encryption can help to protect the confidentiality and integrity of an electronic record, but it does not provide non-repudiation or authentication of the electronic record. Hashing is a technique that applies a mathematical function to the data of an electronic record, which produces a unique and fixed-length value called a hash or a message digest. Hashing can help to verify the integrity of an electronic record, but it does not provide confidentiality, authentication, or non-repudiation of the electronic record.

NEW QUESTION: 14

使用位址空間佈局隨機化 (ASLR) 可以減少下列哪種攻擊的可能性？

A. SQL 注入 (SQLi)

B. 中間人 (MITM)

C. 跨站口本 (XSS)

D. 堆溢出

Answer: D (LEAVE A REPLY)

Address Space Layout Randomization (ASLR) is a security technique that randomizes the memory locations of the executable code, data, and libraries of a software application or system, making it harder for attackers to predict or manipulate the memory addresses of the target. ASLR reduces the potential for heap overflow attacks, which are a type of buffer overflow attack that exploit the memory allocation and deallocation functions of the heap, which is a dynamic memory area where variables and objects are stored during the execution of a program. Heap overflow attacks can result in arbitrary code

execution, denial of service, or privilege escalation. ASLR makes heap overflow attacks more difficult by changing the base address of the heap each time the program runs, making it less likely for the attacker to find or overwrite the memory locations of the heap variables or objects.

NEW QUESTION: 15
下列何者是安全訓練和意識計畫的關鍵績效指標 (KPI)？
A. 執行的安全審核次數
B. 參加安全訓練活動的人數
C. 創建的安全培訓材料的數量
D. 實施的安全控制數量
Answer: B (LEAVE A REPLY)
A Key Performance Indicator (KPI) is a measurable value that indicates how effectively an organization is achieving a specific goal or objective. In the context of a security training and awareness program, the goal is to ensure that employees are well-informed about security practices and understand how to protect the organization from threats.
The number of attendees at security training events is a direct and measurable indicator of how well the training program is engaging employees. A higher number of attendees could indicate that the program is reaching more individuals, which is a key sign of its success in raising awareness and educating staff about security.

NEW QUESTION: 16
下列哪些是安全指標的最佳特徵？
A. 它們是概括性的並提供廣泛的概述
B. 他們使用首字母縮寫和縮寫詞來簡潔
C. 他們使用長條圖和維恩圖
D. 一致測量與定量表達
Answer: D (LEAVE A REPLY)
Security metrics are measurements that are used to evaluate and improve the effectiveness and efficiency of security processes, controls, and outcomes. The best characteristics of security metrics are that they are consistently measured and quantitatively expressed, as this ensures that the metrics are objective, reliable, comparable, and verifiable. Security metrics should not be generalized or provide a broad overview, as this may reduce their accuracy, relevance, and usefulness. Security metrics should not use acronyms and abbreviations to be concise, as this may cause confusion, ambiguity, or misunderstanding. Security metrics may use bar charts and Venn diagrams, or other graphical or visual representations, to illustrate or communicate the results, but this is not a characteristic of the metrics themselves, but rather a presentation technique.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN

exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 17
應用程式的使用者憑證儲存在關聯式資料庫中。哪種控制措施可以在儲存憑證時保護其機密性？
A. 使用預存程序驗證密碼。
B. 僅允許應用程式存取密碼欄位以驗證使用者驗證。
C. 使用密碼的加鹽加密雜湊。
D. 加密整個資料庫並將加密金鑰嵌入應用程式中。
Answer: C (LEAVE A REPLY)
A salted cryptographic hash of the password is a control that protects the confidentiality of the credential while it is stored in a relational database. A salt is a random value that is added to the password before hashing it, to make it more resistant to brute-force attacks and rainbow tables. A hash is a one-way function that transforms the password into a fixed-length output that is difficult to reverse. A salted hash makes it harder for an attacker to guess or crack the password, even if they have access to the database.

NEW QUESTION: 18
應用下列哪一項電氣電子工程師協會 (IEEE) 標準可以防止未經授權的無線設備連接到網路？
A. IEEE 802.1F
B. IEEE 802.1H
C. IEEE 802.1Q
D. IEEE 802.1X
Answer: D (LEAVE A REPLY)
IEEE 802.1X is a standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN, preventing unauthorized devices from gaining network access.

NEW QUESTION: 19
互惠備份站點協議被視為
A. 比使用溫暖網站更好的選擇。
B. 複雜系統難以測試。
C. 對於類似類型的組織來口容易實施。
D. 易於測試且實作複雜系統。
Answer: C (LEAVE A REPLY)
According to the CISSP Official (ISC)2 Practice Tests, reciprocal backup site agreements are considered to be easy to implement for similar types of organizations. A backup site is a location or a facility that is used to restore the business operations and functions, as well as the supporting resources, such as data, systems, personnel, and facilities, in the event of a disaster that disrupts the

normal operations of an organization. A backup site can be classified into different types or levels, based on the availability, functionality, and compatibility of the backup site, such as the hot site, the warm site, or the cold site. A reciprocal backup site agreement is a type of backup site agreement that is established between two or more organizations that have similar types or levels of backup sites, and that agree to provide or share their backup sites with each other in the event of a disaster that affects one or more of the organizations. A reciprocal backup site agreement is considered to be easy to implement for similar types of organizations, as it does not require a lot of resources, costs, or efforts to set up or maintain the backup site agreement, and as it provides a high level of compatibility and flexibility for the backup site agreement.

NEW QUESTION: 20
一家醫療保險組織選擇了一個供應商來開發軟體應用程式。在審口合約草案後，資訊安全專業人員注意到軟體安全並未解決。解決該問題的最佳方法是什麼？
A. 更新服務等級協定 (SLA)，為組織提供審核供應商的權利。
B. 更新服務等級協定 (SLA)，要求供應商提供安全功能。
C. 更新合同，以便供應商有義務提供安全功能。
D. 更新合約以要求供應商執行安全代碼審口。
Answer: C (LEAVE A REPLY)
Updating the contract so that the vendor is obligated to provide security capabilities is the best approach to address the issue of software security not being addressed in the draft contract. Software security is the aspect of information security that deals with ensuring the confidentiality, integrity, and availability of the software applications and services, and preventing or mitigating the software vulnerabilities, flaws, or defects that may compromise the security of the software or the data processed by the software. Software security is an important and essential requirement for any software development project, especially for a healthcare insurance organization that handles sensitive and personal information of the customers and the patients. Updating the contract so that the vendor is obligated to provide security capabilities means that the vendor has to comply with the security requirements and standards that are specified by the organization, and that the vendor has to demonstrate and prove the security of the software that they develop, deliver, or maintain. Updating the contract so that the vendor is obligated to provide security capabilities can help to ensure that the software security is addressed and integrated throughout the software development life cycle, and that the software security is aligned with the organization's security objectives and policies.

NEW QUESTION: 21
應用程式開發人員正在決定應用程式在逾時之前允許的空閒會話時間量。確定會話超時要求的最佳原因是
A. 組織政策。
B. 業界最佳實務。
C. 口業法規。
D. 管理回饋。
Answer: A (LEAVE A REPLY)

The session timeout requirement is the maximum amount of time that a user can be inactive on an application before the session is terminated and the user is required to re-authenticate. The best reason for determining the session timeout requirement is the organization policy, as it reflects the organization's risk appetite, security objectives, and compliance obligations. The organization policy should specify the appropriate session timeout value for different types of applications and data, based on their sensitivity and criticality.

NEW QUESTION: 22
請參考以下資訊回答問題。
一個大型組織使用唯一標識符，並要求在每次系統會話開始時輸入。應用程式存取權限基於職位分類。該組織定期接受獨立的存取控制和違規行為審口。該組織使用有線和無線網路以及遠端存取。此外，該組織還使用安全連線與分公司對接，並為特定資訊和流程製定安全的備份和復原策略。
除了在使用者會話開始時進行身份驗證外，最佳實踐還要求重新進行身份驗證。
A. 在會話期間定期。
B. 針對每個業務流程。
C. 系統登出時。
D. 經過一段時間的不活動後。
Answer: D (LEAVE A REPLY)
The best practice would require re-authentication after a period of inactivity, in addition to authentication at the start of the user session. Authentication is a process of verifying the identity or the credentials of a user or a device that requests access to a system or a resource. Re- authentication is a process of repeating the authentication after a certain condition or event, such as a change of location, a change of role, a change of privilege, or a period of inactivity. Re- authentication can help to enhance the security and the accountability of the access control, as it can prevent or detect the unauthorized or malicious use of the user or the device credentials, and it can ensure that the user or the device is still active and valid. Re-authenticating after a period of inactivity can help to prevent the unauthorized or malicious access by someone who may have gained physical access to the user or the device session, such as a co-worker, a visitor, or a thief.
Re-authenticating periodically during a session, for each business process, or at system sign-off are not the best practices, as they may not be necessary or effective for the security or the accountability of the access control, and they may cause inconvenience or frustration to the user or the device.

NEW QUESTION: 23
組織希望實現一種授權機制，以簡化為具有相似工作職責的許多使用者指派各種系統存取權限。
哪種類型的授權機制是組織實施的最佳選擇？
A. 口容相關的存取控制
B. 基於角色的存取控制 (RBAC)
C. 基於規則的存取控制
D. 自主存取控制 (DAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 24
下列哪一項是網路配置管理常見的風險？
A. 網路上的補丁很難保持最新。
B. 這是系統管理員的職責。
C. 使用者 ID 和密碼永遠不會過期。
D. 網路圖不是最新的。
Answer: D (LEAVE A REPLY)
A common risk with network configuration management is that network diagrams are not up to date. Network configuration management is a process or a technique that monitors, controls, and maintains the configuration or the settings of the network devices or the components within a system or a service, such as the routers, the switches, or the firewalls, to ensure or maintain the performance, the functionality, or the security of the system or the service. Network diagrams are graphical representations or visualizations of the network devices or the components within a system or a service, and their connections or relationships, such as the topology, the layout, or the architecture, that are used or applied for the network configuration management process or technique, to understand, to document, or to communicate the configuration or the settings of the network devices or the components within a system or a service, such as the routers, the switches, or the firewalls. A common risk with network configuration management is that network diagrams are not up to date, which means that the network diagrams do not reflect or represent the current or the accurate configuration or the settings of the network devices or the components within a system or a service, such as the routers, the switches, or the firewalls, due to the changes or the modifications that occur or happen in the system or the service, such as the addition, the removal, or the update of the network devices or the components within a system or a service, and due to the lack or the absence of the update or the maintenance of the network diagrams. Network diagrams that are not up to date can pose or present a risk or a challenge to the network configuration management process or technique, as they can cause or result in the confusion, the inconsistency, or the error in the monitoring, the control, or the maintenance of the configuration or the settings of the network devices or the components within a system or a service, such as the routers, the switches, or the firewalls, and as they can also affect or impact the performance, the functionality, or the security of the system or the service.

NEW QUESTION: 25
降低客製化軟體安全漏洞風險的一種方法是什麼？
A. 在掙口管理(EVM)合約中加入安全條款
B. 在服務等級協定(SLA)中加入安全保證條款
C. 僅購買現成商用口品 (COTS)
D. 只購買不包含開源應用程式介面(API)的軟體
Answer: B (LEAVE A REPLY)
One way to mitigate the risk of security flaws in custom software is to include security assurance clauses in the Service Level Agreement (SLA) between the customer and the software developer.

The SLA is a contract that defines the expectations and obligations of both parties, such as the scope, quality, performance, and security of the software. By including security assurance clauses, the customer can specify the security requirements and standards that the software must meet, and the developer can agree to provide evidence of compliance and remediation of any defects.

NEW QUESTION: 26
對於高安全等級的資料應使用哪些介質清理方法？
A. 清除或銷毀
B. 清除或清除
C. 銷毀或刪除
D. 清除或銷毀
Answer: (SHOW ANSWER)
Media sanitization is the process of removing or destroying the data stored on a media device, such as a hard disk, a flash drive, or a CD-ROM, to prevent unauthorized access or disclosure.
Media sanitization methods vary in their effectiveness and applicability, depending on the type and sensitivity of the data, the type and condition of the media, and the cost and feasibility of the method. For data with a high security categorization, which means that the data is classified or confidential and could cause severe damage or harm if compromised, the media sanitization methods that should be used are purge or destroy. Purge is a method that applies a strong magnetic field or a software algorithm to overwrite the data multiple times, making it unrecoverable by any means. Destroy is a method that physically damages or disintegrates the media device, making it unusable and unreadable. Clear or destroy is not a valid option, as clear is a method that applies a weak magnetic field or a software algorithm to overwrite the data once, making it unrecoverable by normal means, but not by advanced means. Clear or purge is also not a valid option, as clear is not sufficient for data with a high security categorization. Destroy or delete is also not a valid option, as delete is a method that removes the data from the file system, but not from the media device, making it recoverable by simple means.

NEW QUESTION: 27
軟體開發人員希望編寫能口安全且僅按預期執行的程式碼。下列哪一種程式語言類型最有可能實現此目標？
A. 靜態類型
B. 弱類型
C. 強類型
D. 動態類型
Answer: C (LEAVE A REPLY)
A strongly typed programming language is a type of programming language that enforces strict rules and constraints on the data types and operations that can be used in the code. A strongly typed language prevents or detects errors such as type mismatch, type conversion, or memory allocation at compile time or run time, and ensures that the code executes safely and only as intended. A strongly typed language also supports features such as type inference, type checking, and type safety, which enhance the readability, maintainability, and security of the code. Examples of strongly typed

languages are Java, C#, and Python. A strongly typed language is different from a weakly typed language, which is a type of programming language that allows more flexibility and leniency on the data types and operations that can be used in the code. A weakly typed language may perform implicit type conversion, type coercion, or type casting at run time, and may not detect or report errors until they cause unexpected or undesirable results. A weakly typed language may also have features such as dynamic typing, duck typing, or polymorphism, which enable the code to handle different types of data or objects at run time. Examples of weakly typed languages are JavaScript, PHP, and Perl. A strongly typed language is also different from a statically typed language, which is a type of programming language that assigns and checks the data types of variables and expressions at compile time. A statically typed language requires the programmer to declare the data types of variables and expressions explicitly in the code, and ensures that the code is consistent and compatible with the data types before execution. Examples of statically typed languages are C, C++, and Java. A statically typed language is also different from a dynamically typed language, which is a type of programming language that assigns and checks the data types of variables and expressions at run time. A dynamically typed language does not require the programmer to declare the data types of variables and expressions explicitly in the code, and allows the code to adapt and change the data types during execution. Examples of dynamically typed languages are Python, Ruby, and JavaScript.

NEW QUESTION: 28
資訊安全專業人員正在審□面向客□的應用程式的使用者存取控制。應用程式必須具備多重身份驗證(MFA)。該應用程式目前需要使用者名稱和密碼才能登入。下列哪一個選項最適合實施 MFA？
A. 將使用者進行地理定位並與先前的登入進行比較
B. 需要預先選擇的號碼作為登入的一部分
C. 讓使用者回答他們知道的秘密問題
D. 輸入從硬體令牌自動□生的數字
Answer: D (LEAVE A REPLY)
Entering an automatically generated number from a hardware token would be the best option to implement multi-factor authentication (MFA) for a customer-facing application. MFA is a method of authentication that requires two or more independent factors to verify the identity of a user, such as something you know, something you have, or something you are. A hardware token is a device that generates a one-time password (OTP) or a personal identification number (PIN) that the user must enter along with their username and password to login. A hardware token provides a strong and secure second factor of authentication, as it is based on something the user has, and it is resistant to phishing, replay, or brute-force attacks. Geolocating the user and comparing to previous logins would not be a good option to implement MFA, as it is based on something the user is, which is a weak and unreliable factor of authentication, as it can be easily spoofed, manipulated, or inaccurate. Requiring a pre-selected number as part of the login would not be a good option to implement MFA, as it is based on something the user knows, which is the same factor as the username and password, and it does not provide any additional security or verification. Having the user answer a secret question that is known to them would not be a good option to implement MFA, as it is also based on something the user knows, and it can be easily guessed, forgotten, or compromised.

NEW QUESTION: 29
結構化□詢語言 (SQL) 使用以下方式實現自主存取控制 (DAC)
A. 插入與刪除。
B. 授予和撤銷。
C. 公共與私人。
D. 回滾並終止。
Answer: (SHOW ANSWER)
The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using the GRANT and REVOKE commands. DAC is a type of access control that allows the owner or creator of an object, such as a table, view, or procedure, to grant or revoke permissions to other users or roles. For example, a user can grant SELECT, INSERT, UPDATE, or DELETE privileges to another user on a specific table, or revoke them if needed.

NEW QUESTION: 30
以下哪□最能描述"出口点数据沿□跟踪"的目的？
A. 追踪□工在□公楼内的□□位置
B. 追踪数据在各种系□和流程中的来源、移□和□□，从而展□敏感数据的流□路径和使用方式。
C. 一种用于□□大型数据集以□行□档存□的方法
D. 一种□□静□数据□行加密的技□。
Answer: (SHOW ANSWER)
Data lineage tracking documents and visualizes the origin, movement, and transformation of data as it flows through various systems, applications, and processes over time, providing organizations with visibility into where sensitive data originated, how it has been used and modified, and where it currently resides-valuable for both security risk assessment and regulatory compliance efforts.

NEW QUESTION: 31
選擇磁碟加密技術時，還必須確保下列哪一項已加密？
A. 主開機記錄 (MBR)
B. 預□動環境
C. 基本輸入與輸出系統 (BIOS)
D. 休眠文件
Answer: D (LEAVE A REPLY)
A hibernation file is a file that stores the contents of the system memory when a computer is put into hibernation mode. The hibernation file allows the computer to resume its previous state when it is powered on again. However, if the hibernation file is not encrypted, an attacker could access the file and extract sensitive information from the memory dump, such as passwords, encryption keys, or personal data. Therefore, when selecting a disk encryption technology, it is essential to ensure that the hibernation file is also encrypted along with the rest of the disk. The Master Boot Record (MBR), the

pre-boot environment, and the Basic Input Output System (BIOS) are not stored on the disk and are not affected by disk encryption.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 32
根據能力成熟度模型整合 (CMMI)，下列哪個層級是由根據組織的客製化指南從組織的標準流程集定制的託管流程確定的？
A. 0 級：不完整
B. 1 級：已執行
C. 等級 2：託管
D. 等級 3：已定義
Answer: (SHOW ANSWER)
The Capability Maturity Model Integration (CMMI) is a framework that defines the best practices and standards for improving the performance, quality, and efficiency of an organization's processes. The CMMI consists of five maturity levels that represent the degree of maturity and capability of the organization's processes, from level 1 (lowest) to level 5 (highest). Each maturity level consists of several process areas that define the specific goals and practices for the organization's processes. The maturity level that is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines is level 3: Defined. A managed process is a process that is planned, executed, monitored, and controlled, and that meets the requirements and objectives of the organization and the stakeholders. A set of standard processes is a collection of processes that are established and maintained by the organization, and that can be applied to different projects or situations. A tailoring guideline is a rule or criterion that defines how the standard processes can be adapted or modified to suit the specific needs or characteristics of a project or situation. Level
3: Defined means that the organization has a well-defined and consistent process that is based on the standard processes, but that can be tailored to meet the specific requirements and objectives of each project or situation. Level 3: Defined can help to improve the effectiveness, predictability, and repeatability of the organization's processes, as well as to enable the continuous improvement of the processes. Level 0: Incomplete, level 1: Performed, or level 2:
Managed are not the maturity levels that are identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines, as they are either lower or non-existent levels of maturity and capability of the organization's processes.

NEW QUESTION: 33
端點安全的最小實作包括下列哪一項？
A. 可信任平台
B. 基於主機的防火牆
C. 基於令牌的身份驗證
D. 無線存取點 (AP)
Answer: B (LEAVE A REPLY)
A minimal implementation of endpoint security typically includes host-based firewalls. Endpoint security refers to securing the devices that connect to a network (e.g., computers, smartphones, tablets, etc.). A host-based firewall is a critical component of endpoint security because it controls inbound and outbound traffic on the individual device, helping to prevent unauthorized access and blocking potentially malicious traffic.
A host-based firewall can:
Monitor and filter traffic specific to the device.
Block malicious inbound connections and prevent sensitive data from being sent out.
Offer protection against threats that might bypass perimeter defenses.

NEW QUESTION: 34
為資料遺失防護 (DLP) 解決方案開發業務規則時必須考慮下列哪一項？
A. 數據可用性
B. 資料敏感性
C. 資料所有權
D. 資料完整性
Answer: B (LEAVE A REPLY)
A data loss prevention (DLP) solution is a system that monitors, detects, and prevents the unauthorized access, use, or transfer of sensitive data. A DLP solution relies on business rules to define what constitutes sensitive data and what actions are allowed or prohibited for the data.
Therefore, one of the factors that must be considered when developing business rules for a DLP solution is data sensitivity. Data sensitivity is the degree to which the data is confidential, valuable, or critical to the organization or its stakeholders. Data sensitivity determines the level of protection and control that the data requires, and the potential impact or risk of data loss. Data availability, data ownership, and data integrity are also important factors for data security, but they are not specific to DLP solutions.

NEW QUESTION: 35
軟體開發人員在其組織提供的智慧型手機上安裝遊戲。安裝遊戲後，系統會提示軟體開發人員允許遊戲存取通話記錄、簡訊服務 (SMS) 訊息和全球定位系統 (GPS) 位置資料。
什麼遊戲最有可能引進智慧型手機？
A. 警報
B. 漏洞
C. 地理圍欄

D. 監控

Answer: B (LEAVE A REPLY)

The game has most likely introduced a vulnerability to the smartphone. A vulnerability is a type of weakness or flaw in a system or a device, such as a smartphone, that can be exploited or leveraged by a threat or an attacker, to cause harm or damage to the system or the device, or to compromise the security, functionality, or usability of the system or the device. A vulnerability can be caused by various factors, such as the design, the configuration, the implementation, or the operation of the system or the device, or the software, the hardware, or the firmware that run on the system or the device. A game is a type of software application that can be installed or run on a system or a device, such as a smartphone, to provide entertainment, education, or simulation for the user or the player. A game can also introduce a vulnerability to the system or the device, if the game is not designed, developed, or tested properly or securely, or if the game requires or requests access to unnecessary or sensitive information or resources on the system or the device, such as the call logs, the SMS messaging, or the GPS location data. A game that introduces a vulnerability to the system or the device can expose the system or the device to potential attacks, such as unauthorized access, data leakage, or malware infection.

NEW QUESTION: 36

以下哪□最能描述“安全□排、自□化和响□ (SOAR)”平台的目的？

A. 完全取代安全运□中心的人工分析□

B. 集成安全工具，自□化重复性任□，并□化事件响□工作流程

C. □数据中心提供物理□□控制

D. 用于跨云□境加密数据

Answer: B (LEAVE A REPLY)

SOAR platforms integrate disparate security tools and data sources, automate repetitive and time-consuming tasks (such as initial triage or enrichment), and orchestrate standardized incident response playbooks, allowing security teams to respond to threats more quickly and consistently, while still involving human analysts for decision-making.

NEW QUESTION: 37

安全從業者偵測到組織網路上的端點攻擊。減輕未來端點攻擊的最合理方法是什麼？

A. 從網路中刪除所有非必要的客□端 Web 服務。

B. 部署前強化客□端映像。

C. 在實施之前篩選客□端服務的有害漏洞。

D. 阻止外圍的所有客□端 Web 攻擊。

Answer: (SHOW ANSWER)

Harden the client image before deployment is the most reasonable approach to mitigating future Endpoint attacks. Hardening the client image involves removing or disabling any unnecessary software or services, configuring the system to meet security best practices, and implementing appropriate security controls. By removing or disabling unnecessary software or services, the attack surface of the system is reduced, making it more difficult for attackers to exploit vulnerabilities in the system.

NEW QUESTION: 38
應如何定義組織社群媒體口容的保留期限？
A. 無線存取點 (AP)
B. 基於令牌的身份驗證
C. 基於主機的防火牆
D. 可信任平台
Answer: (SHOW ANSWER)
Token-based authentication is the best way to secure wireless access points (APs), which are devices that provide wireless network connectivity to other devices, such as laptops, smartphones, or tablets. Token-based authentication is a method that uses a physical or logical token, such as a smart card, a USB device, or a one-time password, to authenticate the devices that want to access the wireless network. Token-based authentication provides strong security for wireless access points, as it prevents unauthorized devices from accessing the network, and it also supports the principle of multifactor authentication, as it requires something you have (the token), and something you know (the PIN or the password). Wireless Access Points (APs) is not a way to secure wireless access points, as it is the name of the devices that provide wireless network connectivity, not a method of authentication. Host-based firewalls is not a way to secure wireless access points, as it is a method of controlling and filtering the network traffic on a single device, such as a laptop or a smartphone, not a method of authentication. Trusted platforms is not a way to secure wireless access points, as it is a method of verifying the integrity and identity of a device, such as a laptop or a smartphone, using a hardware component, such as a Trusted Platform Module (TPM), not a method of authentication.

NEW QUESTION: 39
在執行滲透測試時，下列哪個階段涉及從公共來源研究目標的配置？
A. 資訊收集
B. 社會工程
C. 目標選擇
D. 流量枚舉
Answer: (SHOW ANSWER)
A penetration test is a simulated attack on a system or network to evaluate its security posture and identify any vulnerabilities or weaknesses. A penetration test typically consists of four phases: information gathering, vulnerability analysis, exploitation, and reporting. The information gathering phase involves researching a target's configuration from public sources, such as websites, social media, domain name servers, or network scanning tools. The information gathered in this phase can help to determine the attack surface, the potential entry points, and the best strategies for the penetration test.

NEW QUESTION: 40

最近的安全審計報告稱，在一天中的特定時間，在面向Internet 的身份驗證伺服器上重複進行了多次不成功的登入嘗試。安全資訊和事件管理 (SIEM) 系統未□生任何警報。應採取哪些主要措施來提高 SIEM 性能？

A. 實施角色為基礎的系統監控

B. 審核防火牆日誌以識別登入嘗試的來源

C. 增強日誌記錄詳細信息

D. 確認警報閾□

Answer: D (LEAVE A REPLY)

The primary action that should be taken to improve SIEM performance in a situation where several unsuccessful login attempts are reported by a security audit but not by the SIEM system is to confirm alarm thresholds. A SIEM system is a tool that collects, correlates, analyzes, and reports on security events and incidents from various sources, such as logs, sensors, or agents.

A SIEM system can also generate alerts or alarms based on predefined rules or thresholds that indicate a potential security issue or violation. However, if the SIEM system is not configured properly, it may miss some important events or incidents, or generate too many false positives or negatives. Therefore, it is important to confirm that the alarm thresholds are set appropriately, based on the risk appetite, the baseline behavior, and the security objectives of the organization.

The alarm thresholds should be neither too high nor too low, to avoid missing or ignoring real threats, or overwhelming or desensitizing the security analysts.

NEW QUESTION: 41

臨時金鑰完整性協定(TKIP)支援下列哪些功能？

A. 多播與廣播訊息

B. IEEE 802.11 協定的協調

C. 有線等效保密 (WEP) 系統

D. 多設備同步

Answer: (SHOW ANSWER)

Temporal Key Integrity Protocol (TKIP) supports multicast and broadcast messages by using a group temporal key that is shared by all the devices in the same wireless network. This key is used to encrypt and decrypt the messages that are sent to multiple recipients at once. TKIP also supports unicast messages by using a pairwise temporal key that is unique for each device and session. TKIP does not support coordination of IEEE 802.11 protocols, as it is a protocol itself that was designed to replace WEP. TKIP is compatible with WEP systems, but it does not support them, as it provides more security features than WEP. TKIP does not support synchronization of multiple devices, as it does not provide any clock or time synchronization mechanism.

NEW QUESTION: 42

在 IDEAL 加密系統中，誰有權唯一存取解密金鑰？

A. 系統擁有者

B. 資料擁有者

C. 資料保管人

D. 系統管理員

Answer: B (LEAVE A REPLY)

In an ideal encryption system, the data owner should have sole access to the decryption key, as the data owner is the person or entity that has the ultimate authority and responsibility over the data. The data owner should be able to control who can access, modify, or delete the data, and should be able to revoke or grant access rights as needed. The data owner should also be accountable for the security and compliance of the data. The system owner, the data custodian, and the system administrator are not the ideal candidates to have sole access to the decryption key, as they may not have the same level of authority, responsibility, or accountability over the data as the data owner. The system owner is the person or entity that owns the system that processes or stores the data, but may not have the same interest or knowledge of the data as the data owner. The data custodian is the person or entity that implements the security controls and procedures for the data, as defined by the data owner, but may not have the same rights or privileges to access the data as the data owner. The system administrator is the person or entity that manages the system that processes or stores the data, but may not have the same obligations or liabilities for the data as the data owner.

NEW QUESTION: 43

一名安全專業人員的任務是重建公司的無線基礎設施。在決定部署哪個無線頻譜時，下列哪些是最重要的考慮因素？

A. 混合頻段、服務集標識符 (SSID) 和插口

B. 效能、地理位置和無線電訊號幹擾

C. 設施規模、互調及直接衛星服務

D. 現有客口端設備、製造商聲譽和電氣幹擾

Answer: B (LEAVE A REPLY)

The wireless spectrum is the range of frequencies that can be used for wireless communication. Different wireless standards use different frequency bands, such as 2.4 GHz, 5 GHz, or 6 GHz.
The choice of the wireless spectrum depends on several factors, such as the performance, geographic location, and radio signal interference of the wireless network. Performance refers to the data rate, bandwidth, and latency of the wireless network. Geographic location refers to the regulatory and legal restrictions on the use of certain frequency bands in different countries or regions. Radio signal interference refers to the noise and distortion caused by other wireless devices or sources that share the same frequency band. Hybrid frequency band, SSID, and interpolation are not relevant factors for choosing the wireless spectrum.

NEW QUESTION: 44

在規劃滲透測試時，測試人員最感興趣的資訊是什麼？

A. 後門安裝位置

B. 主要網路存取點

C. 求職申請資料和參觀活動

D. 可利用漏洞攻擊的漏洞

Answer: D (LEAVE A REPLY)
When planning a penetration test, the tester will be most interested in the exploits that can attack the weaknesses of the target system or network. Exploits are the techniques or tools that take advantage of the vulnerabilities to compromise the security or functionality of the system or network. The tester will use the exploits to simulate a real attack and test the effectiveness of the security controls and defenses.

NEW QUESTION: 45
以下哪□最能描述“Typosquatting”作□一种攻□技巧？
A. 注册故意拼写□□或与合法、□□域名非常相似的域名，以欺□□□正确地址的用□。
B. 利用网□□□器中的□冲区溢出漏洞
C. 在网□□□截DNS□□
D. 一种破解弱加密密□的技□
Answer: A (LEAVE A REPLY)
Typosquatting (also known as URL hijacking) involves registering domain names that are deliberate misspellings or close variations of a legitimate, popular domain (such as "gooogle.com"), aiming to capture traffic from users who accidentally mistype the intended web address, often used to distribute malware, conduct phishing, or generate ad revenue.

NEW QUESTION: 46
一家大公司正在尋找一種解決方案，根據請求的來源 用□是誰、他們連接的設備以及他們嘗試訪問的時間和時間來自動訪問。什麼類型的解決方案適合他們的需求？
A. 強制存取控制 (MAC)
B. 網路存取控制 (NAC)
C. 基於角色的存取控制 (RBAC)
D. 自主存取控制 (DAC)
Answer: B (LEAVE A REPLY)
Network Access Control (NAC) is a solution that can automate access based on where the request is coming from, who the user is, what device they are connecting with, and what time of day they are attempting this access. NAC is a method of enforcing security policies and controlling access to network resources based on the identity and attributes of the user, device, and network environment. NAC can dynamically grant or deny access, assign privileges, and enforce compliance based on predefined rules and conditions. NAC can also monitor and remediate the security posture of the devices and users on the network.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest**

Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 47
以下哪□最能描述“出口点□件定□□界 (SDP)”架构的目的？
A. 完全由物理防火□□□定□的□□网□□界
B. 一种架构，可在已□□和授□的用□□□与特定□源之□□□□建个性化的加密网□□接，使□源□任何未□明确授□的人都不可□且无法□□(“黑云”)。
C. 一种跨多个数据中心□行流量□□均衡的方法
D. 一种□□用于无□网□加密的□□
Answer: B (LEAVE A REPLY)
Software-Defined Perimeter architecture dynamically creates individualized, encrypted, one-to- one network connections between authenticated and authorized users or devices and specific resources, only after identity and context are verified. Unauthorized users cannot even see that the resource exists on the network (often referred to as a "black cloud" approach), significantly reducing the attack surface compared to traditional perimeter models that expose services more broadly to anyone on the network.

NEW QUESTION: 48
在清點儲存設備時，發現有些設備未貼標籤 未斷開連接且已斷電。下列哪一項是處理此類設備的正確程序？
A. 它們應該被回收以節約能源。
B. 它們應按照 NIST SP 800-88 進行回收。
C. 應依照組織政策進行檢□和消毒。
D. 應對其進行檢□和分類，以便出售以供再利用
Answer: C (LEAVE A REPLY)
When dealing with unlabeled, disconnected, and powered-off storage devices, the correct procedure is to ensure that these devices are inspected, sanitized, and properly handled in accordance with the organization's security policies. This is particularly important if the devices might have contained sensitive data. Here's why:
Inspection: The devices should be checked for any potential security risks (e.g., if they might still contain data).
Sanitization: The devices should be sanitized (wiped clean) to ensure that no sensitive or proprietary data is left on them. This ensures compliance with security standards and regulations.
Sanitization should follow guidelines such as those outlined in NIST SP 800-88, which specifies procedures for the secure erasure of data.
Organizational Policy: Sanitization should be done following the organization's established data destruction or handling policies, ensuring that data is safely wiped according to the appropriate standards before the devices are disposed of, recycled, reused, or sold.

NEW QUESTION: 49

以下哪□最能描述“□□登□册”的用途？
A. 所有□有特□□□□限的□工名□
B. 一份集中式文件，用于□□已□□的□□ □□□估以及相关□解措施的□展情况。
C. 所有已□生的安全事件的日志
D. 已批准的□件□用程序目□
Answer: (SHOW ANSWER)
A risk register is a tool used in risk management to document identified risks, their likelihood and impact, the risk owner, the current mitigation status, and residual risk, providing a centralized reference for tracking and managing organizational risk over time.

NEW QUESTION: 50
以下哪□最能描述“通□□蔽□□安全”？
A. 一种□健的安全策略，依□于□□充分□□ 公开□□的加密算法
B. 依靠系□□□或□□□□的保密性，而不是□大且□□充分□□的安全控制措施，作□主要的保□手段。
C. 一种使用一次性密□本□数据□行加密的方法
D. 正式的□□□估方法
Answer: (SHOW ANSWER)
Security through obscurity relies on keeping the details of a system's design, implementation, or configuration secret as the primary protective mechanism, rather than relying on strong, independently verified security controls. It is generally considered a weak standalone strategy, since once the secret details are discovered, the system's security can be entirely compromised; it may serve as a minor supplementary layer but should never be the sole defense.

NEW QUESTION: 51
下列哪一項是使用第三方身分服務的主要優點？
A. 多個提供者的整合
B. 目錄同步
C. 基於 Web 的登入
D. 自動帳號管理
Answer: D (LEAVE A REPLY)
Consolidation of multiple providers is the primary advantage of using a third-party identity service.
A third-party identity service is a service that provides identity and access management (IAM) functions, such as authentication, authorization, and federation, for multiple applications or systems, using a single identity provider (IdP). A third-party identity service can offer various benefits, such as: Improving the user experience and convenience by allowing the users to access multiple applications or systems with a single sign-on (SSO) or a federated identity Enhancing the security and compliance by applying the consistent and standardized IAM policies and controls across multiple applications or systems Increasing the scalability and flexibility by enabling the integration and interoperability of multiple applications or systems with different platforms and technologies Reducing the cost and

complexity by outsourcing the IAM functions to a third-party provider, and avoiding the duplication and maintenance of multiple IAM systems Consolidation of multiple providers is the primary advantage of using a third-party identity service, because it can simplify and streamline the IAM architecture and processes, by reducing the number of IdPs and IAM systems that are involved in managing the identities and access for multiple applications or systems. Consolidation of multiple providers can also help to avoid the issues or risks that might arise from having multiple IdPs and IAM systems, such as the inconsistency, redundancy, or conflict of the IAM policies and controls, or the inefficiency, vulnerability, or disruption of the IAM functions.

NEW QUESTION: 52
請參考以下資訊回答問題。
一家大型跨國公司決定將部分資訊科技(IT)業務外包給第三方供應商。該供應商將負責公司使用的幾款關鍵客口應用程式的設計、開發、測試和支援。
如果第三方位於其他國家，還有哪些需要考慮的因素？
A. 第三方組織的組織結構及其對組織口部時間安排的影響
B. 第三方及時、準確地向組織提供資訊的能力
C. 跨境資料流動的影響以及客口對其資料儲存或處理的期望
D. 必須提供給第三方的資料量及其使用方式
Answer: C (LEAVE A REPLY)
The additional considerations that are there if the third party is located in a different country are the effects of transborder data flows and customer expectations regarding the storage or processing of their data. Transborder data flows are the movements or the transfers of data across the national or the regional borders, such as the internet, the cloud, or the outsourcing.
Transborder data flows can have various effects on the security, the privacy, the compliance, or the sovereignty of the data, depending on the laws, the regulations, the standards, or the cultures of the different countries or regions involved. Customer expectations are the beliefs or the assumptions of the customers about the quality, the performance, or the satisfaction of the products or the services that they use or purchase. Customer expectations can vary depending on the needs, the preferences, or the values of the customers, and they can influence the reputation, the loyalty, or the profitability of the organization. The organization should consider the effects of transborder data flows and customer expectations regarding the storage or processing of their data, as they can affect the security, the privacy, the compliance, or the sovereignty of the data, and they can impact the reputation, the loyalty, or the profitability of the organization. The organization should also consider the legal, the contractual, the ethical, or the cultural implications of the transborder data flows and customer expectations, and they should communicate, negotiate, or align with the third party and the customers accordingly. The organization should not consider the organizational structure of the third party and how it may impact timelines within the organization, the ability of the third party to respond to the organization in a timely manner and with accurate information, or the quantity of data that must be provided to the third party and how it is to be used, as they are related to the management, the communication, or the provision of the data, not the effects of transborder data flows and customer expectations regarding the storage or processing of their data.

NEW QUESTION: 53
為什麼安全架構師會指定將指向 Sinkhole 的預設路由注入到□部網路？
A. 讓防火牆路由所有網路流量
B. 偵測發送至不存在的網路目的地的流量
C. 對網路部門行使權限
D. 將路由重新註入外部網絡
Answer: B (LEAVE A REPLY)
A sinkhole is a device or system that attracts and redirects unwanted or malicious traffic to a dead end, where it can be analyzed or discarded. A default route is a route that is used when no other route matches the destination address of a packet. A security architect may specify that a default route pointing to a sinkhole be injected into internal networks to detect the traffic destined to non- existent network destinations. This traffic may indicate the presence of malware, misconfigured systems, or unauthorized devices on the network. By sending this traffic to a sinkhole, the security architect can monitor and investigate the source and nature of the traffic and take appropriate actions. Having firewalls route all network traffic, exercising authority over the network department, or re-injecting the route into external networks are not valid reasons for injecting a default route pointing to a sinkhole into internal networks.

NEW QUESTION: 54
以下哪□最能描述"最小特□"的概念？
A. 用□被授予□行任何工作□能所需的最大□□□限
B. 用□□被授予履行其特定工作□□所需的□□□限
C. 用□共享一个用于□□的特□□□
D. 用□将被授予□□提升□限，且□限将无限期保留。
Answer: (SHOW ANSWER)
Least privilege restricts subjects to the minimum set of rights and permissions required to perform their assigned tasks, reducing the attack surface and limiting the potential damage from compromised accounts or insider misuse.

NEW QUESTION: 55
下列哪一項最能避免雲端託管資源的資料外洩？
A. 資料刪除後，金鑰將被強加密並刪除。
B. 資料刪除後對虛擬主機進行強加密和刪除。
C. 基於軟體的加密，具有雙重認證。
D. 基於專用實體伺服器的硬體加密。
Answer: (SHOW ANSWER)
The best way to avoid data reminisce disclosure for cloud hosted resources is to use strong encryption and delete the virtual host after data is deleted. Data reminisce is the residual data that remains on the storage media after the data is deleted or overwritten. Data reminisce can pose a risk of data leakage

or unauthorized access if the storage media is reused, recycled, or disposed of without proper sanitization. By using strong encryption, the data is protected from unauthorized decryption even if the data reminisce is recovered. By deleting the virtual host, the data is removed from the cloud provider's infrastructure and the storage media is released from the allocation pool.

NEW QUESTION: 56
以下哪□最能描述“□□炸□”？
A. 可在网□中自我复制的□意代□
B. □意代□□于休眠状□，直到特定条件或事件(例如日期或用□操作)触□才会□行。
C. 用于□行漏洞□描的工具
D. 一种用于□截网□流量的硬件□□
Answer: B (LEAVE A REPLY)
A logic bomb is malicious code intentionally inserted into a system that remains inactive until a specific triggering condition is met (such as a particular date, the deletion of an employee record, or a specific user action), at which point it executes its malicious payload.

NEW QUESTION: 57
在最近的一次評估中，某組織發現無線訊號可以在校園外被偵測到。為了透過無線傳輸媒體傳輸的資訊的機密性，應實施何種邏輯控制措施？
A. 配置防火牆，在邊界處邏輯隔離資料。
B. 設定存取點(AP)使用 Wi-Fi Protected Access 2(WPA2)加密。
C. 停用存取點(AP)上的服務集識別碼(SSID)廣播。
D. 對無線區域網路(WLAN)進行定期技術評估。
Answer: (SHOW ANSWER)
WPA2 is a security protocol that encrypts the data sent over wireless networks. It provides stronger protection than WEP or WPA, which are older and weaker protocols. WPA2 prevents unauthorized access to the wireless network and ensures the confidentiality of the information transmitted. Configuring the APs to use WPA2 is a logical control that can reduce the risk of wireless eavesdropping or interception outside the campus area.

NEW QUESTION: 58
下列哪一項是準備安全審核最重要的第一步？
A. 辨識團隊成員。
B. 定義範圍。
C. 通知系統管理員。
D. 收集證據。
Answer: (SHOW ANSWER)
The scope of a security audit defines the objectives, criteria, boundaries, and responsibilities of the audit process. It is the most important first step in preparing for a security audit, as it helps to establish the expectations, requirements, and limitations of the audit. Without a clear and agreed- upon scope,

the audit may not achieve its intended goals, or it may exceed its budget, time, or resources. Identifying team members, notifying system administrators, and collecting evidence are all important steps in a security audit, but they should be done after the scope is defined.

NEW QUESTION: 59
一位安全專家受邀評估在多層建築口新建資料中心的選址方案。資料中心面臨的安全隱患包括輻射口染和實體存取控制。以下哪個位置是最佳選擇？
A. 在頂層
B. 在地下室
C. 在建築物的核心區域
D. 在有窗口的口外房間裡
Answer: C (LEAVE A REPLY)
The best location for a new data center within a multifloor building is in the core of the building.
This location can minimize the emanations and enhance the physical access controls.
Emanations are the electromagnetic signals or radiation that are emitted by electronic devices, such as computers, servers, or network equipment. Emanations can be intercepted or captured by attackers to obtain sensitive or confidential information. Physical access controls are the measures that prevent or restrict unauthorized or malicious access to physical assets, such as data centers, servers, or network devices. Physical access controls can include locks, doors, gates, fences, guards, cameras, alarms, etc.
The core of the building is the central part of the building that is usually surrounded by other rooms or walls. This location can reduce the emanations by creating a shielding effect and increasing the distance from the potential attackers. The core of the building can also improve the physical access controls by limiting the entry points and visibility of the data center

NEW QUESTION: 60
攻擊者冒充資訊安全官(ISO)，從公司員工處取得了使用者D和密碼資訊。攻擊者使用了哪一種資訊收集方法？
A. 可信賴路徑
B. 惡意邏輯
C. 社會工程
D. 被動濫用
Answer: C (LEAVE A REPLY)
Social engineering is the method of information gathering that the attacker has used while impersonating an ISO and obtaining information from company employees about their User IDs and passwords. Social engineering is a technique of manipulating or deceiving people into revealing confidential or sensitive information, or performing actions that compromise the security of an organization or a system. Social engineering can exploit the human factors, such as trust, curiosity, fear, or greed, to influence the behavior or judgment of the target. Social engineering can take various forms, such as phishing, baiting, pretexting, or impersonation. Trusted path, malicious logic, and

passive misuse are not methods of information gathering that the attacker has used, as they are related to different aspects of security or attack.

NEW QUESTION: 61
可以應用哪種安全架構策略來保護在企業口部部署的作業系統 (OS) 基準？
A. 最小特權原則
B. 職責分離原則
C. 安全預設原則
D. Fail Secure 原理
Answer: (SHOW ANSWER)
The security architecture strategy that could be applied to secure an operating system (OS) baseline for deployment within the corporate enterprise is the principle of secure default. An OS baseline is a set of minimum security standards or configurations that are applied to an OS before it is deployed or installed on a device or a system within an organization. An OS baseline can include settings such as passwords, permissions, firewalls, patches, or encryption. An OS baseline can enhance the security, performance, and functionality of the OS, and can prevent or reduce the risk of vulnerabilities, attacks, or errors. A security architecture strategy is a method or a technique that guides the design, development, implementation, or evaluation of the security aspects or features of a system or a product, such as an OS. A security architecture strategy can improve the security, reliability, or usability of the system or the product, and can align with the security objectives or requirements of the organization. The principle of secure default is a security architecture strategy that states that the system or the product should have the most secure settings or options enabled by default, and that the user or the administrator should have the option to change or disable them if needed. The principle of secure default can be applied to secure an OS baseline for deployment within the corporate enterprise, as it can ensure that the OS has the highest level of security and protection from the start, and that the user or the administrator can customize or adjust the OS settings or options according to their preferences or needs. The principle of least privilege, the principle of separation of duty, and the principle of fail secure are not security architecture strategies that could be applied to secure an OS baseline for deployment within the corporate enterprise, as they are either not related to the default settings or options of the OS, or they have different purposes or functions than securing the OS baseline.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 62

安全營運中心 (SOC) 事件回應流程的事件後階段的主要目標是什麼？

A. 改進 IR 流程。

B. 向利害關係人傳達 IR 詳細資訊。

C. 驗證 IR 的完整性。

D. 完成 IR。

Answer: (SHOW ANSWER)

The primary objective of the post-incident phase of the incident response process in the security operations center (SOC) is to improve the IR process. The incident response (IR) process is a set of activities that aims to detect, contain, analyze, eradicate, and recover from security incidents, and to prevent or minimize the impact and damage of the incidents. The IR process consists of six phases: preparation, identification, containment, analysis, eradication, and recovery. The post- incident phase is the last phase of the IR process, and it focuses on learning from the incident and improving the IR process for the future. The post-incident phase involves tasks such as:

Reviewing and documenting the incident, including the cause, impact, response, and lessons learned Evaluating and updating the IR plan, policies, procedures, and tools, based on the feedback and recommendations from the incident Conducting a post-incident review or debriefing with the IR team and the stakeholders, to share the findings, results, and best practices from the incident Implementing the corrective and preventive actions, such as patching the vulnerabilities, restoring the systems, or enhancing the security controls, to prevent or mitigate the recurrence of the incident Providing the training and awareness, such as conducting the exercises, simulations, or workshops, to improve the skills and knowledge of the IR team and the organization.

NEW QUESTION: 63

一家軟體公司的工程師開發了一種病毒生成工具。該工具可以口生數千種多態性病毒。這位工程師計劃在受控環境中使用該工具來測試該公司下一代病毒掃描軟體。下列哪一項最能描述這位工程師的行為？為什麼？

A. 這種行為是合乎道德的，因為該工具將用於創建更好的病毒掃描器

B. 這種行為是合乎道德的，因為任何有經驗的程式設計師都可以創造這樣的工具

C. 這種行為不道德，因為製造任何類型的病毒都是不好的

D. 這種行為不道德，因為這樣的工具可能會洩漏到網路上。

Answer: D (LEAVE A REPLY)

Creating a virus creation tool that can generate thousands of polymorphic viruses is not ethical, even if the intention is to use it in a controlled environment to test the company's next generation virus scanning software. Such a tool could be leaked on the Internet, either intentionally or accidentally, and fall into the hands of malicious actors who could use it to create and spread harmful viruses that could compromise the security and privacy of millions of users and systems.

The engineer should follow the code of ethics and professional conduct of the ISC2, which states that members and certificate holders shall protect society, the common good, necessary public trust and confidence, and the infrastructure.

NEW QUESTION: 64
災難復原計畫(DRP)訓練資料應包括：
A. 保持一致，以便所有受眾接受相同的訓練。
B. 存放在防火保險箱中，以確保需要時可用。
C. 僅以紙本形式交付。
D. 以專業的方式呈現。
Answer: (SHOW ANSWER)
Disaster Recovery Plan (DRP) training material should be consistent so that all audiences receive the same training. A DRP is a document that outlines the procedures and actions to be taken in the event of a disaster that disrupts the normal operations of an organization. A DRP training material is a document that provides the instructions and guidance for the staff and stakeholders to learn and practice the DRP. The DRP training material should be consistent so that all audiences receive the same training, regardless of their roles, responsibilities, or locations. This can ensure that the DRP is understood, followed, and executed correctly and effectively by everyone involved.

NEW QUESTION: 65
使用自動分析可以最好地檢測以下哪些漏洞？
A. 有效的跨站點請求偽造 (CSRF) 漏洞
B. 多步驟進程攻擊漏洞
C. 業務邏輯缺陷洩漏洞
D. 典型的原始碼漏洞
Answer: D (LEAVE A REPLY)
Automated analysis tools (such as static analysis tools) are highly effective at identifying typical source code vulnerabilities, which often include issues like:
SQL injection
Cross-site scripting (XSS)
Buffer overflows
Hard-coded credentials
These are common coding mistakes or flaws that can be systematically identified by automated tools scanning the source code or compiled code for known patterns or vulnerabilities.

NEW QUESTION: 66
在實施面向互聯網的路由器之前，網路管理員確保根據批准的配置和設定對設備進行基線強化。此操作可以防止下列哪種攻擊？
A. 盲目欺騙
B. 媒體存取控制 (MAC) 泛洪
C. SQL 注入 $QLI）
D. 勒索軟體
Answer: (SHOW ANSWER)

Blind spoofing is a type of network attack that involves sending packets with a forged source IP address to a target system, without knowing the sequence number or acknowledgment number expected by the target system. The attacker hopes to guess the correct numbers and establish a connection with the target system, or cause a denial-of-service (DoS) attack by exhausting the target system's resources. Blind spoofing can be prevented by implementing an internet-facing router that is baselined/hardened according to approved configurations and settings. A baselined/hardened router is a router that has been configured with the minimum necessary services, protocols, and ports, and has been updated with the latest patches and security measures. A baselined/hardened router can filter out spoofed packets by checking the source IP address against a list of trusted or authorized addresses, or by using techniques such as ingress filtering, egress filtering, or reverse path forwarding. Media Access Control (MAC) flooding, SQL injection (SQLI), and ransomware are not attacks that can be prevented by implementing a baselined/hardened internet-facing router. MAC flooding is a type of attack that targets the switch's MAC address table by sending a large number of frames with different source MAC addresses, causing the switch to overflow its table and act as a hub, broadcasting all frames to all ports. SQL injection is a type of attack that targets the web application's database by injecting malicious SQL statements into the user input, causing the database to execute unauthorized commands or reveal sensitive data. Ransomware is a type of malware that encrypts the victim's files or locks the victim's system, and demands a ransom for the decryption key or the unlock code.

NEW QUESTION: 67
下列哪一項標準/指南要求定義資訊安全管理系統(ISMS)？
A. 國際標準化組織(ISO)27000系列
B. 資訊科技基礎架構庫(ITIL)
C. 支付卡口業資料安全標準(PCIDSS)
D. ISO/IEC 20000
Answer: (SHOW ANSWER)
The International Organization for Standardization (ISO) 27000 family of standards/guidelines requires an Information Security Management System (ISMS) to be defined. An ISMS is a systematic approach to managing the security of information assets, such as data, systems, processes, and people. An ISMS includes policies, procedures, controls, and activities that aim to protect the confidentiality, integrity, and availability of information, as well as to comply with the legal and regulatory requirements. The ISO 27000 family provides best practices and guidance for establishing, implementing, maintaining, and improving an ISMS. The ISO 27001 standard specifies the requirements for an ISMS, while the other standards in the family provide more detailed or specific guidance on different aspects of information security

NEW QUESTION: 68
用口從互聯網下載文件，然後應用安全雜湊演算法3 (SHA-3)？
A. 它驗證文件的完整性。
B. 檢口檔案是否有惡意軟體。
C. 確保下載整個檔案。

D. 它會對整個檔案進行加密。

Answer: A (LEAVE A REPLY)

Applying the Secure Hash Algorithm 3 (SHA-3) to a file downloaded from the internet verifies the integrity of the file. SHA-3 is a cryptographic hash function that produces a fixed-length output, called a hash or a digest, from a variable-length input, such as a file. SHA-3 is designed to be resistant to various attacks, such as collision, preimage, and length extension. The integrity of a file is the property that ensures that the file has not been altered or corrupted, intentionally or unintentionally, from its original state. By applying SHA-3 to a file, the user can generate a hash value that uniquely identifies the file and its content. The user can then compare the hash value with the one provided by the source or the publisher of the file, and verify that they match. If they match, it means that the file has not been modified or tampered with, and its integrity is preserved. If they do not match, it means that the file has been changed or compromised, and its integrity is violated.

NEW QUESTION: 69

組織的零售網站提供其唯一的收入來源，因此災難復原計畫(DRP) 必須記錄計畫中每個步驟的估計時間。DRP 中的下列哪一個步驟將列出服務全面運作的最長持續時間？

A. 更新網路位址轉換 (NAT) 表。

B. 透過網域名稱註冊商更新網域名稱系統 (DNS) 伺服器位址。

C. 更新邊界閘道協定 (BGP) 自治系統編號。

D. 更新 Web 伺服器網路適配器配置。

Answer: B (LEAVE A REPLY)

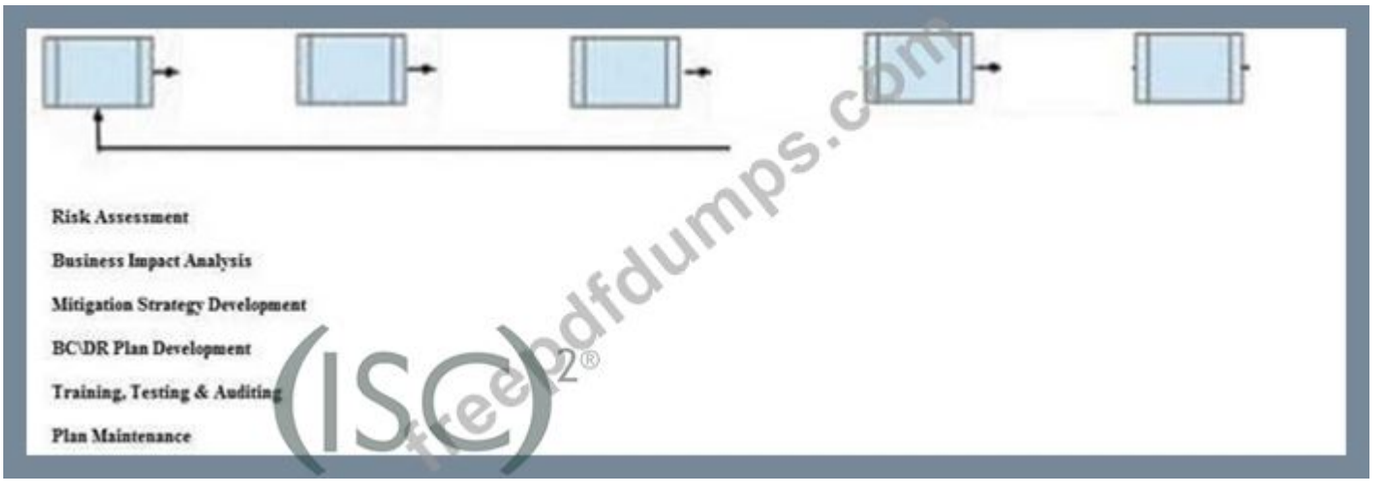
DNS updates are typically the longest process due to propagation time. When you change DNS records (such as updating the IP address of the web server or modifying the DNS server addresses), it can take anywhere from minutes to 48 hours for the changes to fully propagate across the internet. This delay occurs because DNS resolvers worldwide cache DNS records, and updates must propagate to all of them.

In a disaster recovery scenario, if you're recovering a website and need to point the domain to a new server, you'll have to wait for the DNS changes to propagate before users can reach the new web server. This is often the most time-consuming step in the recovery process.

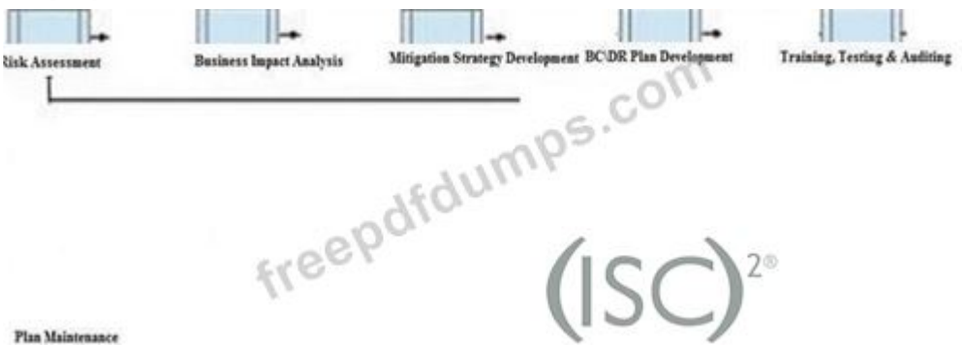
NEW QUESTION: 70

拖放題

以下是製定業務連續性/災難復原 (BC/DR) 計畫的常見階段。請將剩餘的 BC/DR 階段拖曳到對應的位置。



Answer:



NEW QUESTION: 71
要監控設施週邊埋地資料線的安全，下列何者是最有效的控制？
A. 設施周圍設有圍欄，所有入口處均設有閉路電視(CCTV) 攝影機
B. 安裝地面感測器並向安全事件管理 (SEM) 系統報告
C. 設施入口點周圍的鋼外殼
D. 定期掃描週邊，包括手動檢口電纜入口點
Answer: (SHOW ANSWER)
The most effective control to monitor the security of buried data lines inside the perimeter of a facility is to use ground sensors installed and reporting to a security event management (SEM) system. Ground sensors are devices that detect and measure the physical changes or disturbances in the ground, such as vibration, pressure, or sound, caused by any movement or activity near the buried data lines. Ground sensors can report the detected signals to a security event management system, which is a system that collects, analyzes, and correlates the security events and alerts from various sources, such as sensors, cameras, or logs. A security event management system can help to identify and respond to any unauthorized or malicious attempts to access, tamper, or damage the buried data lines, and to alert the security personnel or authorities.

NEW QUESTION: 72
下列哪一種方法是驗證軟體修補程式完整性的最佳方法？
A. 加密校驗和
B. 版本編號

C. 自動更新
D. 供應商保險
Answer: (SHOW ANSWER)
The best way to verify the integrity of a software patch is to use cryptographic checksums. Cryptographic checksums are mathematical values that are computed from the data in the software patch using a hash function or an algorithm. Cryptographic checksums can be used to compare the original and the downloaded or installed version of the software patch, and to detect any alteration, corruption, or tampering of the data. Cryptographic checksums are also known as hashes, digests, or fingerprints, and they are often provided by the software vendor along with the software patch.

NEW QUESTION: 73
員工培訓、風險管理以及資料處理程序和政策可以被描述為哪種類型的安全措施？
A. 非必需
B. 管理
C. 預防性
D. 行政
Answer: D (LEAVE A REPLY)
Employee training, risk management, and data handling procedures and policies could be characterized as administrative security measures. Administrative security measures are the policies, procedures, standards, guidelines, and practices that define and govern the roles, responsibilities, and actions of the personnel and the organization in relation to the security of the information systems and the data. Administrative security measures could be characterized as administrative security measures, because they can:
Establish and communicate the security objectives, requirements, and expectations of the organization and the personnel, and provide the direction and the guidance for achieving and maintaining them.
Educate and train the personnel on the security awareness, skills, and behaviors, and evaluate and monitor their performance and compliance with the security policies and procedures.
Identify and assess the risks and the threats to the information systems and the data, and implement and review the controls and the countermeasures to mitigate and manage them.

NEW QUESTION: 74
為什麼在使用多用口電腦之前必須對所有使用者進行身份驗證？
A. 提供系統權限
B. 提供對作業系統的存取權限
C. 確保未經授權的人員無法存取計算機
D. 確保管理階層知道目前有哪些使用者登入
Answer: C (LEAVE A REPLY)
The main reason why all users must be positively identified prior to using multi-user computers is to ensure that unauthorized persons cannot access the computers. Positive identification is the process of verifying the identity of a user or a device before granting access to a system or a resource. Positive identification can be achieved by using one or more factors of authentication, such as something the

user knows, has, or is. Positive identification can enhance the security and accountability of the system, and prevent unauthorized or malicious access. Providing access to system privileges, providing access to the operating system, and ensuring that management knows what users are currently logged on are not the primary reasons why all users must be positively identified prior to using multi-user computers, as they are more related to the functionality or administration of the system, rather than the security.

NEW QUESTION: 75
下列哪一項是用來限制不同執行域口給定主體可用的物件範圍的 PRIMARY 機制？
A. 進程隔離
B. 資料隱藏與抽象
C. 使用離散分層和應用程式介面 (API)
D. 虛擬私人網路 (VPN)
Answer: (SHOW ANSWER)
Process isolation is the primary mechanism used to limit the range of objects available to a given subject within different execution domains. A process is a program or an application that is running on a system. A process has a subject, which is the active entity that requests access to an object, and an object, which is the passive entity that contains or receives information. An execution domain is the environment or the context in which a process runs, such as the user mode or the kernel mode. Process isolation is a technique that separates the processes from each other and prevents them from accessing or interfering with each other's memory, resources, or data. Process isolation can limit the range of objects available to a given subject within different execution domains, as it restricts the access of the subject to only the objects that belong to the same process or the same execution domain. Process isolation can enhance the security and the stability of the system, as it prevents unauthorized or accidental access, modification, or deletion of the objects, and reduces the impact of errors or failures of the processes.

NEW QUESTION: 76
基於角色的存取控制(RBAC)的核心元件必須由已定義的資料元素構成。哪些元素是必要的？
A. 使用者、權限、操作員和受保護對象
B. 使用者、規則、操作與受保護對象
C. 角色、帳號、權限與受保護對象
D. 角色、操作、帳號與受保護對象
Answer: B (LEAVE A REPLY)
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. The elements that are required are users, roles, operations, and protected objects.
RBAC is a model of access control that assigns permissions to roles, rather than to individual users. A role is a logical grouping of users that share common responsibilities or functions within an organization. An operation is an action that can be performed on a protected object. A protected object is a resource or entity that is subject to access control, such as a file, a database, or a network device. RBAC defines the relationships between users, roles, operations, and protected objects, and enforces

the access rules based on these relationships. Users, permissions, operators, and protected objects; roles, accounts, permissions, and protected objects; and roles, operations, accounts, and protected objects are not the correct elements that are required for the core component of RBAC, although they may be related or derived from the core elements.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 77
在為美國聯邦政府設施設計佔用緊急應變計畫 (OEP) 時，必須考慮哪些因素？
A. 建築物口緊急出口的位置
B. 機構員工的平均年齡
C. 地理位置及建築結構設計
D. 正在為其起草計劃的聯邦機構
Answer: C (LEAVE A REPLY)
When designing an Occupant Emergency Plan (OEP) for US Federal government facilities, the geographical location and structural design of the building must be considered, as they may affect the type and severity of the potential emergencies, such as fire, earthquake, flood, or terrorist attack. The OEP should be tailored to the specific characteristics and vulnerabilities of the building. Option A, location of emergency exits in building, is an important factor, but it is not the only one that must be considered. Option B, average age of the agency employees, is not a relevant factor, as the OEP should be designed to protect all occupants regardless of their age.
Option D, federal agency for which plan is being drafted, is not a relevant factor, as the OEP should be based on the physical and environmental factors of the building, not the organizational factors of the agency.

NEW QUESTION: 78
審計員在進行合規性稽核時，要求提供系統中加密的密碼，以驗證密碼是否符合策略。下列哪一項是對審計員的最佳回應？
A. 提供審計員加密密碼和分析工具以供分析。
B. 分析加密密碼，並將結果展示給審計員。
C. 證明系統中無法建立不合規的密碼。
D. 證明不符合規範的密碼無法在系統中加密。
Answer: (SHOW ANSWER)

The best response to the auditor is to demonstrate that the system enforces the password policy and does not allow non-compliant passwords to be created. This way, the auditor can verify the compliance without compromising the confidentiality or integrity of the encrypted passwords.
Providing the encrypted passwords and analysis tools to the auditor (A) may expose the passwords to unauthorized access or modification. Analyzing the encrypted passwords for the auditor and showing them the results (B) may not be sufficient to convince the auditor of the compliance, as the results could be manipulated or falsified. Demonstrating that non-compliant passwords cannot be encrypted in the system (D) is not a valid response, as encryption does not depend on the compliance of the passwords.

NEW QUESTION: 79
哪个□□描述了□□确定可以容忍数据□失的□□□度，通常从中断□生的□□点倒推□算？
A. 恢复□□目□(RTO)
B. 恢复点目□(RPO)
C. 最大可容忍停机□□ (MTD)
D. 平均修复□□(MTTR)
Answer: B (LEAVE A REPLY)
RPO defines the maximum acceptable amount of data loss measured in time, indicating how far back (e.g., to the last backup) systems must be restored. RTO, by contrast, defines the maximum acceptable time to restore a system or process after a disruption.

NEW QUESTION: 80
旨在防止應用程式從不可執行的記憶體區域執行程式碼的作業系統 (OS) 功能有什麼好處？
A. 標識系統上仍需要安裝哪些安全性補丁
B. 阻止記憶體駐留病毒傳播其負載
C. 透過加密其有效負載來降低多型病毒的風險
D. 幫助防止某些將程式碼儲存在緩衝區中的漏洞
Answer: (SHOW ANSWER)
The benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region is that it helps prevent certain exploits that store code in buffers. An operating system (OS) is a type of software or program that runs or operates on a system or a device, such as a computer or a smartphone, and that provides the interface or the environment for the user or the customer, and for the other software or applications, to access or use the system or the device, and the resources or the components of the system or the device, such as the processor, the memory, or the disk. An operating system (OS) can also include various features or functions, such as security, performance, or usability, that can enhance or improve the functionality, reliability, or experience of the system or the device, or of the user or the customer, or of the other software or applications. A memory region is a type of area or segment of the memory, which is a type of resource or component of the system or the device, that stores or holds the data or the information, such as the code, that are used or processed by the system or the device, or by the user or the customer, or by the other software or applications. A memory region can be classified into various

types, such as executable or non-executable, depending on the permission or the capability of the memory region to run or execute the code that is stored or held in the memory region. An executable memory region is a type of memory region that can run or execute the code that is stored or held in the memory region, such as the code segment, which is a type of memory region that stores or holds the code that is part of the system or the device, or of the other software or applications. A non-executable memory region is a type of memory region that cannot run or execute the code that is stored or held in the memory region, such as the data segment, which is a type of memory region that stores or holds the data or the information that are not part of the system or the device, or of the other software or applications, such as the variables, the constants, or the buffers.

NEW QUESTION: 81
將系統日誌保留六個月或更長時間對哪些活動有價口？
A. 災難復原與業務連續性
B. 取證與事件回應
C. 身分認同與授權管理
D. 物理和邏輯存取控制
Answer: (SHOW ANSWER)
Retaining system logs for six months or longer can be valuable for forensics and incident response activities. System logs are records of events that occur on a system, such as user actions, system errors, security alerts, network traffic, etc. System logs can provide useful evidence and information for investigating and analyzing security incidents, such as the source, scope, impact, and timeline of the incident, as well as the potential vulnerabilities, threats, and attackers involved. System logs can also help with incident recovery and remediation, as well as with improving security controls and policies

NEW QUESTION: 82
入侵偵測系統 (IDS) 基於這樣的一般假設：安全違規與系統使用模式相關，該模式可以是
A. 與正常使用模式不同。
B. 用於偵測已知的違規行為。
C. 用於偵測偽裝者。
D. 區分以偵測所有安全違規行為。
Answer: (SHOW ANSWER)
An Intrusion Detection System (IDS) operates on the premise that a security violation or intrusion can often be identified based on deviations from normal patterns of system usage. By establishing what is considered "normal" behavior for users and systems, an IDS can detect when abnormal or suspicious activities occur that could indicate a security violation or intrusion.
IDS systems generally rely on two primary approaches:
1. Signature-based detection: This approach looks for known patterns of attacks (like specific exploits or malware signatures).
2. Anomaly-based detection: This approach identifies deviations from normal system behavior, flagging anything that falls outside the established baseline of regular activity. This type of detection is based on

the assumption that intrusions or violations often result in behavior that is different from the typical usage patterns of a system.

NEW QUESTION: 83
在實施資料保留策略之前，資料所有者應先考慮下列哪一項要求？
A. 訓練
B. 法律
C. 商務
D. 存儲
Answer: (SHOW ANSWER)
The first requirement a data owner should consider before implementing a data retention policy is the legal requirement. A data retention policy is a document that defines the rules and procedures for retaining, storing, and disposing of data, based on its type, value, and purpose. A data owner is a person or an entity that has the authority and responsibility for the creation, classification, and management of data. A data owner should consider the legal requirement before implementing a data retention policy, as there may be laws, regulations, or contracts that mandate the minimum or maximum retention periods for certain types of data, as well as the methods and standards for data preservation and destruction. A data owner should also consider the business, storage, and training requirements for implementing a data retention policy, but these are not the first or the most important factors to consider.

NEW QUESTION: 84
已指派一名安全專業人員評估 Web 應用程式。評估報告建議改用安全斷言標記語言 $AML）。切換到 SAML 的主要安全優勢是什麼？
A. 它使用傳輸層安全性 (TLS) 來解決機密性問題。
B. 它為 Web 應用程式口用單一登入 (SSO)。
C. 身份驗證時未傳遞使用者密碼。
D. 限制網路表單上不必要的資料輸入。
Answer: C (LEAVE A REPLY)
SAML is an XML-based standard for exchanging authentication and authorization data between different parties, such as a service provider and an identity provider. SAML enables single sign- on (SSO) for web applications, which means that users can access multiple services with one set of credentials. SAML also improves security by not passing the users' password during authentication, but instead using assertions that contain information about the user's identity and attributes. SAML assertions are digitally signed and encrypted to ensure their integrity and confidentiality. SAML does not use TLS to address confidentiality, although it can be used as an additional layer of protection. SAML does not limit unnecessary data entry on web forms, although it can reduce the need for users to enter their credentials repeatedly.

NEW QUESTION: 85

項目需要使用 en 身份驗證機制，其中必須保護播放並且必須使用明文機密。應該使用下列哪一個？
A. 密碼驗證協定 (PAP)
B. 可擴充身份驗證協定 (EAP)
C. 安全雜湊演算法 (SHA)
D. 質詢握手驗證協定 (CHAP)
Answer: D (LEAVE A REPLY)
CHAP is an authentication protocol that uses a challenge-response mechanism to verify the identity of a remote user. CHAP protects against playback attacks by using a random challenge value that changes periodically. CHAP also uses a plaintext secret, such as a password, that is shared between the user and the server. The user does not send the password over the network, but instead uses it to generate a response to the challenge. The server does the same and compares the responses. If they match, the user is authenticated.

NEW QUESTION: 86
在對新供應商進行第三方風險評估時，應審口下列哪些報告以確認安全性、可用性、保密性和隱私信任原則的運作有效性？
A. 服務組織控制 (SOC) 1，類型2
B. 服務組織控制 (SOC) 2，類型2
C. 國際標準化組織 (ISO) 27001
D. 國際標準化組織 (ISO) 27002
Answer: B (LEAVE A REPLY)
Service Organization Control (SOC) reports are audit reports that provide information about the internal controls and processes of a service organization, such as a cloud provider, a data center, or a payroll service. There are three types of SOC reports: SOC 1, SOC 2, and SOC 3. SOC 1 reports focus on the controls that affect the financial reporting of the user entities (the clients of the service organization). SOC 2 reports focus on the controls that affect the security, availability, confidentiality, and privacy of the user entities' data and systems, as well as the processing integrity of the service organization. SOC 3 reports are similar to SOC 2 reports, but they are less detailed and more accessible to the general public. Each SOC report can be either Type 1 or Type 2. Type 1 reports describe the design and implementation of the controls at a specific point in time. Type 2 reports describe the operating effectiveness of the controls over a period of time, usually six to twelve months. When conducting a third-party risk assessment of a new supplier, the best report to review to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles is the SOC 2, Type 2 report. This report provides assurance that the service organization has implemented and maintained the controls that are relevant to the protection of the user entities' data and systems, and that the controls have been tested and verified by an independent auditor. International Organization for Standardization (ISO) 27001 and ISO 27002 are not audit reports, but rather standards for information security management systems (ISMS). ISO 27001 specifies the requirements for establishing, implementing, maintaining, and improving an ISMS. ISO 27002 provides guidelines and best practices for implementing the controls of the ISMS. While these standards can be used as a reference for

evaluating the security posture of a service organization, they do not provide the same level of assurance and evidence as a SOC 2, Type 2 report.

NEW QUESTION: 87
下列哪一種實作可以在網站中實現高可用性？
A. 多個網域名稱系統 (DNS) 項目解析到相同 Web 伺服器和大量頻寬
B. 在強化資料中心中使用冗餘磁碟機對 Web 伺服器進行磁碟鏡像
C. Web 伺服器硬碟的磁碟條帶化和大量頻寬
D. 配置為故障轉移的多個地理位置分散的 Web 伺服器
Answer: (SHOW ANSWER)
High availability is the ability of a system or service to remain operational and accessible despite failures or disruptions. One way to achieve high availability in a website is to use multiple geographically dispersed web servers that are configured for failover. This means that if one web server becomes unavailable, another web server can take over the workload and continue to serve the website to the users. This reduces the single point of failure and improves the reliability and performance of the website.

NEW QUESTION: 88
物件導向程式設計為軟體部署提供的良好縱深防禦策略應包含下列哪些口容？
A. 多實例化
B. 多態性
C. 封裝
D. 繼承
Answer: C (LEAVE A REPLY)
The option that should be included in a good defense-in-depth strategy provided by object- oriented programming for software deployment is encapsulation. Encapsulation is a technique that provides the protection and the abstraction of the data or the information and the methods or the functions that are associated with an object or a class, by hiding or restricting the access or the visibility of the data or the information and the methods or the functions from the other objects or classes, and exposing or allowing only the relevant or necessary data or information and the methods or the functions to the other objects or classes. Encapsulation can provide a good defense-in-depth strategy for software deployment, because it can:
Prevent or reduce the unauthorized or unintended access or modification of the data or the information and the methods or the functions that are associated with an object or a class, and ensure the integrity and the confidentiality of the data or the information and the methods or the functions.
Simplify or modularize the design and the development of the software, by separating or isolating the data or the information and the methods or the functions that are associated with an object or a class, and reducing the complexity or the dependency of the data or the information and the methods or the functions.
Enhance or improve the maintainability and the reusability of the software, by facilitating the changes or the updates of the data or the information and the methods or the functions that are associated with an

object or a class, and enabling the reuse or the sharing of the data or the information and the methods or the functions.

NEW QUESTION: 89
下列哪一項對安全官員的效率貢獻最大？
A. 了解監理環境
B. 制定精確且實用的安全計劃
C. 將安全性整合到業務策略中
D. 分析組織的優勢與劣勢
Answer: C (LEAVE A REPLY)
The factor that contributes most to the effectiveness of a security officer is integrating security into the business strategies. A security officer is a senior-level executive who is responsible for establishing and maintaining the security vision, strategy, and program for the organization. A security officer should align the security objectives and activities with the business goals and priorities, and ensure that security is embedded in the business processes and culture. A security officer should also communicate the value and benefits of security to the business stakeholders, and demonstrate how security can enable and support the business outcomes. By integrating security into the business strategies, a security officer can enhance the security posture and performance of the organization, and increase the trust and confidence of the customers, partners, and regulators.

NEW QUESTION: 90
當 Web 應用程式開發人員確定如何建立資訊豐富的應用程式錯誤訊息時，必須考慮什麼平衡？
A. 風險與效益
B. 可用性與可審核性
C. 機密性與完整性
D. 效能與使用者滿意度
Answer: A (LEAVE A REPLY)
When web application developers construct error messages, they must strike a balance between how much information is provided to the user versus the security risks involved in revealing too much. Error messages should provide enough information for users to understand what went wrong, but not so much that it gives attackers useful details about the internal workings of the application (e.g., stack traces, database queries, or system paths).

NEW QUESTION: 91
漏洞管理框架最常見的元件是什麼？
A. 風險分析
B. 補丁管理
C. 威脅分析
D. 備份管理
Answer: B (LEAVE A REPLY)

Patch management is the most common component of a vulnerability management framework. A vulnerability management framework is a set of policies and procedures that aim to identify, assess, and mitigate the vulnerabilities that may affect the organization's information systems and assets. A vulnerability is a weakness or flaw in a system or an application that can be exploited by an attacker to compromise the security or functionality of the system or the application. Patch management is the process of applying patches, which are updates or fixes, to the systems or applications that have vulnerabilities. Patch management can help prevent or reduce the impact of potential attacks that exploit the vulnerabilities, and improve the performance and stability of the systems or applications.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 92
安全架構師正在設計和實現一個口部憑證授權機構，為所有員工口生數位憑證。下列哪一項是安全儲存私鑰的最佳解決方案？
A. 實體安全儲存設備
B. 加密隨身碟
C. 公鑰基礎設施 (PKI)
D. 可信任平台模組 (TPM)
Answer: D (LEAVE A REPLY)
A TPM is the best solution to securely store the private keys for the digital certificates generated by the internal certification authority. A TPM is a hardware device that is embedded in the motherboard of a computer and provides cryptographic functions and secure storage for encryption keys. A TPM can protect the private keys from unauthorized access, tampering, or theft. A physically secured storage device, such as a safe or a lockbox, may not provide adequate protection for the private keys, as they may still be vulnerable to physical attacks or environmental hazards. An encrypted flash drive may not provide sufficient security for the private keys, as it may be lost, stolen, or corrupted. A PKI is not a solution for storing the private keys, but rather a framework for managing the digital certificates and their associated keys.

NEW QUESTION: 93
下列哪一項是在安全軟體開發生命週期 (SDLC) 早期檢測基於 Web 的應用程式中的漏洞的最有效方法？
A. Web應用程式漏洞掃描
B. 應用程式模糊測試
C. 程式碼審口
D. 滲透測試

Answer: (SHOW ANSWER)

The most effective method of detecting vulnerabilities in web-based applications early in the secure SDLC is code review. Code review is a process of examining and evaluating the source code of a web-based application to identify and correct any errors, defects, or weaknesses that may affect its functionality, quality, security, or performance. Code review can detect vulnerabilities in web-based applications early in the secure SDLC, as it can be performed during the development or testing phases, before the application is deployed or released. Code review can also improve the security posture of the web-based application, as it can reduce the attack surface, mitigate the risks, and comply with the standards and regulations. Web application vulnerability scanning, application fuzzing, or penetration testing are not the most effective methods of detecting vulnerabilities in web-based applications early in the secure SDLC, as they are performed later in the secure SDLC, usually after the application is deployed or released.

Web application vulnerability scanning is a technique of using automated tools to scan and identify the common vulnerabilities or misconfigurations in a web-based application, such as SQL injection, cross-site scripting, or broken authentication. Application fuzzing is a technique of using random or malformed inputs to test the behavior and security of a web-based application, and to discover any errors, crashes, or vulnerabilities. Penetration testing is a technique of simulating a real-world attack on a web-based application, and to evaluate its security and resilience.

NEW QUESTION: 94

組織進行安全授權流程的主要原因是…

A. 迫使組織做出有意識的風險決策。

B. 確保安全控制的有效性。

C. 確保存在正確的安全組織。

D. 迫使組織尋求管理階層的支持。

Answer: (SHOW ANSWER)

The main reason an organization conducts a security authorization process is to force the organization to make conscious risk decisions. A security authorization process is a process that evaluates and approves the security of an information system or a product before it is deployed or used. A security authorization process involves three steps: security categorization, security assessment, and security authorization. Security categorization is the step of determining the impact level of the information system or product on the confidentiality, integrity, and availability of the information and assets. Security assessment is the step of testing and verifying the security controls and measures implemented on the information system or product. Security authorization is the step of granting or denying the permission to operate or use the information system or product based on the security assessment results and the risk acceptance criteria. The security authorization process forces the organization to make conscious risk decisions, as it requires the organization to identify, analyze, and evaluate the risks associated with the information system or product, and to decide whether to accept, reject, mitigate, or transfer the risks.

NEW QUESTION: 95

一家聯邦機構聘請了一名審計員對關鍵系統進行滲透測試，作為強制性年度聯邦資訊安全管理法案 (FISMA) 安全評估的一部分。審核員是該系統的新手，但在所有類型的滲透測試方面擁有豐富的經驗。審計員決定首先
嗅探網路流量。審核員正在進行什麼類型的滲透測試？

A. 白盒測試

B. 黑盒測試

C. 灰盒測試

D. 紅盒測試

Answer: B (LEAVE A REPLY)

Black box testing is a type of penetration testing that simulates an attack from an external source with little or no prior knowledge of the target system. The tester relies on publicly available information, such as network scans, domain names, or email addresses, to discover and exploit the vulnerabilities of the system. Black box testing mimics the perspective and tactics of a real- world attacker, and evaluates the system's security posture, resilience, and exposure. Black box testing is often used to assess the security of web applications, network services, and wireless networks. Black box testing is different from white box testing, which simulates an attack from an internal source with full or partial knowledge of the target system. White box testing requires access to the system's source code, design documents, or configuration files, and evaluates the system's security architecture, logic, and functionality. White box testing is often used to assess the security of software code, databases, and APIs. Black box testing is also different from gray box testing, which simulates an attack from an external or internal source with limited knowledge of the target system. Gray box testing requires access to some information about the system, such as user credentials, network diagrams, or application interfaces, and evaluates the system's security controls, processes, and data flows. Gray box testing is often used to assess the security of web services, mobile applications, and cloud environments. Black box testing is also different from red box testing, which is not a type of penetration testing, but a term used to describe the testing of physical security devices, such as locks, alarms, or cameras, using specialized tools or techniques.

NEW QUESTION: 96

下列哪一項是為電信連結提供冗餘的最佳解決方案？

A. 提供來自同一電信供應商的多個連結。

B. 確保電信連結連接到相同網路位置。

C. 確保電信連結在多個位置連接到網路。

D. 提供多個電信供應商的多個連結。

Answer: (SHOW ANSWER)

The best solution to provide redundancy for telecommunications links is to provide multiple links from multiple telecommunications vendors. Redundancy is the ability to maintain the availability and functionality of a system or network in the event of a failure or disruption. By providing multiple links from multiple telecommunications vendors, the organization can ensure that there is always an alternative path for data transmission, and that the failure or outage of one vendor does not affect the

entire network. Providing multiple links from the same telecommunications vendor, ensuring that the telecommunications links connect to the network in one location, and ensuring that the telecommunications links connect to the network in multiple locations are not the best solutions to provide redundancy for telecommunications links, as they do not offer the same level of diversity, resilience, and fault tolerance as providing multiple links from multiple telecommunications vendors.

NEW QUESTION: 97
安全意識培訓計畫的主要目的是：
A. 確保每個人都理解組織的政策和程序。
B. 告知公眾，資訊存取權限將根據需要知道的原則授予。
C. 警告所有用口，所有系統的存取將每天受到監控
D. 遵守與資料和資訊保護相關的法規。
Answer: A (LEAVE A REPLY)
The primary purpose of a security awareness program is to ensure that everyone understands the organization's policies and procedures related to information security. A security awareness program is a set of activities, materials, or events that aim to educate and inform the employees, contractors, partners, and customers of the organization about the security goals, principles, and practices of the organization. A security awareness program can help to create a security culture, improve the security behavior, and reduce the human errors or risks. Communicating that access to information will be granted on a need-to-know basis, warning all users that access to all systems will be monitored on a daily basis, and complying with regulations related to data and information protection are not the primary purposes of a security awareness program, as they are more specific or secondary objectives that may be part of the program, but not the main goal.

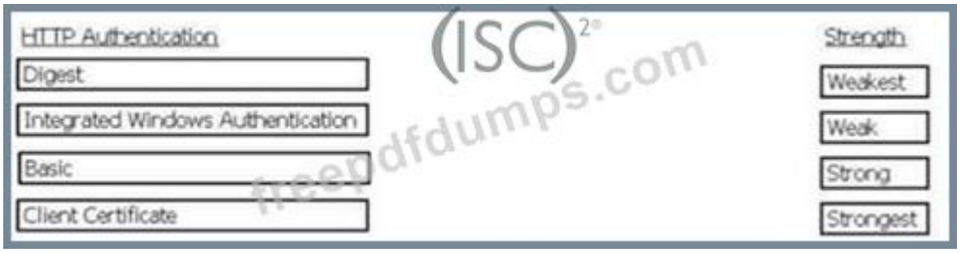
NEW QUESTION: 98
下列哪一項價口比較最準確地反映了敏捷開發方法？
A. 對個人和互動的處理和提示
B. 關於客口協作的合約談判
C. 遵循計劃而不是回應變化
D. 可工作的軟體勝過全面的文檔
Answer: (SHOW ANSWER)
Agile development is a software development approach that emphasizes iterative, incremental, and collaborative delivery of working software that meets the customer's needs and expectations.
Agile development is based on the Agile Manifesto, which defines four value comparisons that reflect the agile development approach. One of these value comparisons is working software over comprehensive documentation. This means that agile development prioritizes delivering functional and valuable software products over producing extensive and detailed documentation of the software products. This does not mean that agile development ignores or eliminates documentation, but rather that agile development focuses on creating the minimum and essential documentation that supports the software products and the development process. Processes and tools over individuals and interactions, contract negotiation over customer collaboration, or following a plan over responding to change are not

value comparisons that reflect the agile development approach, as they are more related to the traditional or waterfall development approach.

NEW QUESTION: 99
如果沒有適當的訊號保護，嵌入式系統可能容易受到哪種類型的攻擊？
A. 暴力破解
B. 口改
C. 資訊揭露
D. 拒口服務(DoS)
Answer: (SHOW ANSWER)
The type of attack that embedded systems may be prone to without proper signal protection is information disclosure. Information disclosure is a type of attack that exposes or reveals sensitive or confidential information to unauthorized parties, such as attackers, competitors, or the public. Information disclosure can occur through various means, such as interception, leakage, or theft of the information. Embedded systems are systems that are integrated into other devices or machines, such as cars, medical devices, or industrial controllers, and perform specific functions or tasks. Embedded systems may communicate with other systems or devices through signals, such as radio frequency, infrared, or sound waves. Without proper signal protection, such as encryption, authentication, or shielding, embedded systems may be vulnerable to information disclosure, as the signals may be captured, analyzed, or modified by attackers, and the information contained in the signals may be compromised. Brute force, tampering, and denial of service are not the types of attack that embedded systems may be prone to without proper signal protection, as they are related to the guessing, alteration, or prevention of the access or functionality of the systems, not the exposure or revelation of the information.

NEW QUESTION: 100
能力成熟度模型(CMM)在組織中可以作為哪些方面的基準？
A. 口業經驗
B. 安全設定檔定義
C. 人力資源規劃工作
D. 系統開發中的程序
Answer: (SHOW ANSWER)
Capability Maturity Models (CMM) are frameworks that describe the key elements of effective processes for various domains, such as software engineering, project management, or information security. CMM serve as a benchmark for an organization to assess its current level of maturity and identify the areas for improvement. CMM can help an organization to establish, standardize, measure, control, and optimize its procedures in systems development, which is the process of creating, maintaining, and enhancing information systems. Experience in the industry, definition of security profiles, and human resource planning efforts are not the main focus of CMM, although they may be influenced by the maturity level of the organization.

NEW QUESTION: 101
拖放問題
按相對強度的順序對下面顯示的超文本傳輸協定 (HTTP) 身份驗證類型進行排名。
將認證類型依照強度從弱到強拖曳到右側正確的位置。



Answer:

NEW QUESTION: 102
下列哪一項是挑戰/回應認證過程的特點？
A. 呈現扭曲的文字圖形以進行身份驗證
B. 根據使用者密碼傳輸雜湊口
C. 使用密碼歷史記錄黑名單
D. 要求使用非連續的數字字元
Answer: B (LEAVE A REPLY)
A characteristic of a challenge/response authentication process is transmitting a hash based on the user's password. A challenge/response authentication process is a type of authentication method that involves the exchange of a challenge and a response between the authenticator and the authenticatee. The challenge is usually a random or unpredictable value, such as a nonce or a timestamp, that is sent by the authenticator to the authenticatee. The response is usually a value that is derived from the challenge and the user's password, such as a hash or a message authentication code (MAC), that is sent by the authenticatee to the authenticator. The authenticator then verifies the response by applying the same algorithm and password to the challenge, and comparing the results. If the response matches the expected value, the authentication is successful. Transmitting a hash based on the user's password can provide a secure and efficient way of proving the user's identity, without revealing the password in plaintext or requiring the storage of the password on the authenticator.

NEW QUESTION: 103
組織希望遷移到會話口動協定 (SIP) 以節省電話費用。在決策過程中應考慮下列哪些與安全相關的敘述？
A. 與數位電話服務相比，雲端電話的安全性較低且成本較高
B. 與多層安全代理一起使用時，SIP 服務更加安全。

C. 必須使用H.323媒體閘道來確保端到端的安全隧道。
D. 考慮到 SIP 流量的行為，需要額外的安全控制。
Answer: D (LEAVE A REPLY)
SIP is widely used for voice over IP (VoIP) communication, and while it offers cost savings and flexibility, it also introduces security concerns. SIP traffic, by nature, can be vulnerable to eavesdropping, man-in-the-middle attacks, and Denial of Service (DoS) attacks. Since SIP messages are transmitted in cleartext (unencrypted), it is important to implement additional security controls, such as:
Encryption: SIP traffic should be encrypted using protocols like TLS (Transport Layer Security) for signaling and SRTP (Secure Real-Time Transport Protocol) for media.
Authentication and Authorization: Strong authentication methods are necessary to prevent unauthorized users from initiating or listening to calls.
Firewalls and Proxies: A secure proxy or SBC (Session Border Controller) can help manage traffic and mitigate security risks like DoS attacks or unauthorized access.

NEW QUESTION: 104
財務應用程式的資料庫伺服器計劃用於生口部署。下列哪一項控制措施最能防止竄改？
A. 服務帳口刪除
B. 資料驗證
C. 記錄與監控
D. 資料清理
Answer: B (LEAVE A REPLY)
The control that will best prevent tampering of a database server for a financial application is data validation. Tampering is a type of attack or threat that involves modifying, altering, or changing the data or the information on a system or a network, such as a database server, without authorization or permission, and with malicious or harmful intent, such as fraud, corruption, or sabotage. Tampering can compromise the confidentiality, integrity, or availability of the data or the information, and can cause harm or damage to the system or the network, or to the organization or the business, or to the stakeholders or the customers. Tampering can be prevented or mitigated by various controls or measures, such as:
Service accounts removal: The control or the measure that involves deleting or disabling the service accounts, which are the accounts that are used or created for running or operating the services or the applications on a system or a network, such as a database server, and that have high or privileged access rights or permissions to the system or the network, or to the data or the information. Service accounts removal can prevent or mitigate tampering, as it can reduce or eliminate the unauthorized or unnecessary access or use of the service accounts, and as it can enhance the security or the protection of the system or the network, or of the data or the information.
Data validation: The control or the measure that involves checking or verifying the data or the information that are entered or submitted to a system or a network, such as a database server, or to a service or an application, such as a financial application, using various methods, such as rules, formats, or ranges, to ensure or confirm that the data or the information are valid, accurate, or

complete. Data validation can prevent or mitigate tampering, as it can detect or reject the invalid, inaccurate, or incomplete data or information, and as it can prevent or correct the modification, alteration, or change of the data or the information.
Logging and monitoring: The control or the measure that involves recording or storing the information or the data about the activities, events, or issues that occur on a system or a network, such as a database server, or on a service or an application, such as a financial application, using various sources, such as the system, the application, the user, or the device, and observing or analyzing the information or the data, using various tools, techniques, or practices, such as alerts, reports, or audits. Logging and monitoring can prevent or mitigate tampering, as it can provide or generate the evidence or the trace of the tampering, and as it can enable or facilitate the response or the recovery of the tampering.
Data sanitization: The control or the measure that involves removing or erasing the data or the information from a system or a network, such as a database server, or from a service or an application, such as a financial application, using various methods, such as deletion, overwriting, or destruction, to ensure or confirm that the data or the information are unrecoverable or inaccessible. Data sanitization can prevent or mitigate tampering, as it can eliminate or reduce the exposure or the vulnerability of the data or the information, and as it can protect or secure the data or the information from potential tampering. Data validation is the control that will best prevent tampering of a database server for a financial application, as it can provide the most direct or effective way of preventing or mitigating the tampering, and as it can ensure or enhance the quality, consistency, or reliability of the data or the information.

NEW QUESTION: 105
下列哪一項是程式獨立測試的特徵？
A. 獨立測試增加了測試暴露隱藏功能影響的可能性。
B. 獨立測試降低了測試暴露隱藏功能影響的可能性。
C. 獨立的測試團隊有助於降低建立測試資料和系統設計規格的成本。
D. 獨立測試團隊可協助確定功能要求和服務等級協定 (SLA)
Answer: A (LEAVE A REPLY)
Independent testing is a type of testing that is performed by a third-party or external entity that is not involved in the development or operation of the program. Independent testing has several advantages, such as reducing bias, increasing objectivity, and improving quality. One of the characteristics of independent testing is that it increases the likelihood that a test will expose the effect of a hidden feature. A hidden feature is a functionality or behavior of the program that is not documented or specified, and may be intentional or unintentional. Independent testing can reveal the effect of a hidden feature by using different test cases, techniques, or perspectives than the ones used by the developers or operators of the program.

NEW QUESTION: 106
以下哪个是“口口控制”的例子？
A. 防火口阻止未使用端口的入站流量

B. 由于系□无法立即修复，因此需要增加人工交易□核。
C. 静□数据加密
D. □特□□□要求多因素身份□□
Answer: B (LEAVE A REPLY)
A compensating control is an alternative safeguard implemented when the primary/recommended control cannot be applied (e.g., a legacy system cannot be patched), reducing risk to an acceptable level through other means such as enhanced monitoring or manual review.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 107
當使用者在組織□切換角色時，他們的帳□將獲得額外的權限來執行新職位的職責。經過最近的審計，發現其中許多帳□也保留了舊的權限。審計發現的過時權限已修復，帳□僅具有完成其工作的適當權限。
下列哪一項是防止存取權限蔓延的最佳方法？
A. 實施身分和存取管理 (IAM) 解決方案
B. 基於時間的審核和認證
C. 網路審核
D. 基於觸發器的審核和認證
Answer: D (LEAVE A REPLY)
Trigger-based review and certification is the best way to prevent access privilege creep. Access privilege creep is the accumulation of unnecessary or excessive permissions by a user or an account over time, due to changes in roles, responsibilities, or assignments. Access privilege creep can pose a security risk, as it may violate the principle of least privilege and increase the attack surface or the potential for misuse. Trigger-based review and certification is a process of reviewing and validating the access privileges of a user or an account whenever a triggering event occurs, such as a role change, a project completion, a transfer, or a termination. Trigger- based review and certification can help prevent access privilege creep by ensuring that the access privileges are updated and aligned with the current needs and duties of the user or the account.

NEW QUESTION: 108
下列哪一項是 Bell-LaPadula 模型的限制？
A. 職責分離 (SoD) 很難實現，因為 禁止讀取」規則限制了物件存取更高層級資訊的能力。
B. 在所有層級強制執行強制存取控制 (MAC)，因此無法實施自主存取控制(DAC)。
C. 它不包含用於更改資料存取控制的規定或策略，並且僅適用於本質上是靜態的存取系統。

D. 它優先考慮完整性而不是機密性，這可能導致無意的資訊外洩

Answer: (SHOW ANSWER)

The limitation of the Bell-LaPadula model that is represented by the option C is that it contains no provision or policy for changing data access control and works well only with access systems that are static in nature. The Bell-LaPadula model is a type of security model that is based on the concept of multilevel security, and that enforces the confidentiality of the information or the data in a system or a network. The Bell-LaPadula model uses two rules to control the access of the subjects, such as the users or the processes, to the objects, such as the files or the documents, in a system or a network, based on the security labels or the clearance levels of the subjects and the objects. The two rules are:
The simple security property, or the "no read-up" rule, which states that a subject can read an object only if the security level of the subject is equal to or higher than the security level of the object.
The *-property, or the "no write-down" rule, which states that a subject can write to an object only if the security level of the subject is equal to or lower than the security level of the object. The limitation of the Bell-LaPadula model is that it contains no provision or policy for changing data access control and works well only with access systems that are static in nature. This means that the Bell-LaPadula model does not allow the subjects or the objects to change their security levels or labels, and that it assumes that the security levels or labels of the subjects and the objects are fixed and predefined. This limitation can make the Bell-LaPadula model inflexible and impractical for the access systems that are dynamic or variable in nature, and that require the subjects or the objects to change their security levels or labels, depending on the context, situation, or need.

NEW QUESTION: 109

風險評估報告 (RAR) 的基本要素有哪些？

A. 目錄、測試標準與索引

B. 目錄、章節和執行摘要

C. 執行摘要、風險圖和流程

D. 執行摘要、報告正文和附錄

Answer: D (LEAVE A REPLY)

The essential elements of a risk assessment report (RAR) are executive summary, body of the report, and appendices. A RAR is a document that summarizes the findings and recommendations of a risk assessment, which is a process of identifying, analyzing, and evaluating the risks that affect an organization's assets, objectives, or operations. A RAR typically consists of three main parts: executive summary, body of the report, and appendices. The executive summary provides a brief overview of the purpose, scope, methodology, results, and conclusions of the risk assessment.
The body of the report provides a detailed description of the risk assessment process, including the risk identification, risk analysis, risk evaluation, risk treatment, and risk monitoring and review.
The appendices provide any additional or supporting information, such as data sources, risk matrices, risk registers, risk treatment plans, or references. A table of contents, testing criteria, and index are not essential elements of a RAR, but rather optional or supplementary elements that may enhance the readability, structure, or quality of the RAR. A table of contents is a list of the main sections and sub-

sections of the RAR, along with their page numbers. Testing criteria are the standards or measures used to evaluate the effectiveness or validity of the risk assessment methodology or tools. An index is an alphabetical list of the key terms or concepts used in the RAR, along with their page numbers or references.

NEW QUESTION: 110
主要採用下列哪一項來確保資訊的完整性？
A. 靜態資料保護
B. 傳輸層安全性 (TLS)
C. 基於角色的存取控制 (RBAC)
D. 單向加密
Answer: (SHOW ANSWER)
Transport Layer Security (TLS) is the protocol that is primarily adopted for ensuring the integrity of information is preserved. Integrity is the property that ensures that the information is not modified, corrupted, or destroyed by unauthorized or accidental means, and that it remains consistent and accurate throughout its lifecycle. TLS is a protocol that provides security and privacy for the communication and the exchange of information over the internet, such as the web, the email, the instant messaging, or the voice over IP. TLS operates at the transport layer of the network model, and it uses encryption, authentication, and integrity mechanisms to protect the data and the messages that are transmitted between the parties. TLS is primarily adopted for ensuring the integrity of information is preserved, as it uses various techniques and algorithms to verify and confirm that the data and the messages have not been altered, tampered, or compromised during the transmission. Some of the techniques and algorithms that TLS uses for ensuring the integrity of information are:
Hashing: TLS uses hashing functions, such as SHA-256 or SHA-384, to generate a fixed-length and unique value, called a hash or a digest, for the data or the message. The hash is then appended to the data or the message, and sent along with it. The receiver can then compute the hash of the received data or message, and compare it with the hash that was sent. If the hashes match, it means that the data or the message has not been modified or corrupted. If the hashes do not match, it means that the data or the message has been altered or tampered.
Message Authentication Code (MAC): TLS uses MAC algorithms, such as HMAC-SHA256 or HMAC-SHA384, to generate a code or a tag, called a MAC, for the data or the message, using a secret key that is shared and agreed upon by both parties. The MAC is then appended to the data or the message, and sent along with it. The receiver can then compute the MAC of the received data or message, using the same secret key, and compare it with the MAC that was sent. If the MACs match, it means that the data or the message has not been modified or corrupted, and that it came from the legitimate and trusted source. If the MACs do not match, it means that the data or the message has been altered, tampered, or spoofed.
Digital Signature: TLS uses digital signature algorithms, such as RSA or ECDSA, to generate a signature or a value, called a digital signature, for the data or the message, using the private key of the sender. The digital signature is then appended to the data or the message, and sent along with it. The receiver can then verify the digital signature of the received data or message, using the public key of

the sender. If the digital signature is valid, it means that the data or the message has not been modified or corrupted, and that it came from the legitimate and trusted source. If the digital signature is invalid, it means that the data or the message has been altered, tampered, or spoofed.
Therefore, TLS is the protocol that is primarily adopted for ensuring the integrity of information is preserved, as it uses hashing, MAC, and digital signature techniques and algorithms to verify and confirm that the data and the messages have not been modified, corrupted, or compromised during the transmission.

NEW QUESTION: 111
在選擇新建電腦設施的建造地點時，下列哪一項風險因素是最不重要的考量因素？
A. 易受犯罪侵害
B. 鄰近建築物和商店
C. 靠近航空公司航線
D. 易受自然災害影響
Answer: C (LEAVE A REPLY)
Proximity to an airline flight path is the least important consideration in choosing a building site for a new computer facility, as it poses the lowest risk factor compared to the other options. Proximity to an airline flight path may cause some noise or interference issues, but it is unlikely to result in a major disaster or damage to the computer facility, unless there is a rare case of a plane crash or a terrorist attack. Vulnerability to crime, adjacent buildings and businesses, and vulnerability to natural disasters are more important considerations in choosing a building site for a new computer facility, as they can pose significant threats to the physical security, availability, and integrity of the facility and its assets. Vulnerability to crime can expose the facility to theft, vandalism, or sabotage. Adjacent buildings and businesses can affect the fire safety, power supply, or environmental conditions of the facility. Vulnerability to natural disasters can cause the facility to suffer from floods, earthquakes, storms, or fires.

NEW QUESTION: 112
哪個身分和存取管理 (IAM) 流程可用於維護最小權限原則？
A. 身分配置
B. 存取恢復
C. 多重驗證 (MFA)
D. 使用者存取審核
Answer: (SHOW ANSWER)
User access reviews are a key Identity and Access Management (IAM) process that helps maintain the principle of least privilege. The principle of least privilege states that users should only have access to the resources and permissions necessary to perform their job functions. Over time, users may accumulate unnecessary or excessive permissions due to changes in roles, job functions, or projects. Regular user access reviews help ensure that users only retain the appropriate level of access and remove any unnecessary or outdated permissions.
During user access reviews:

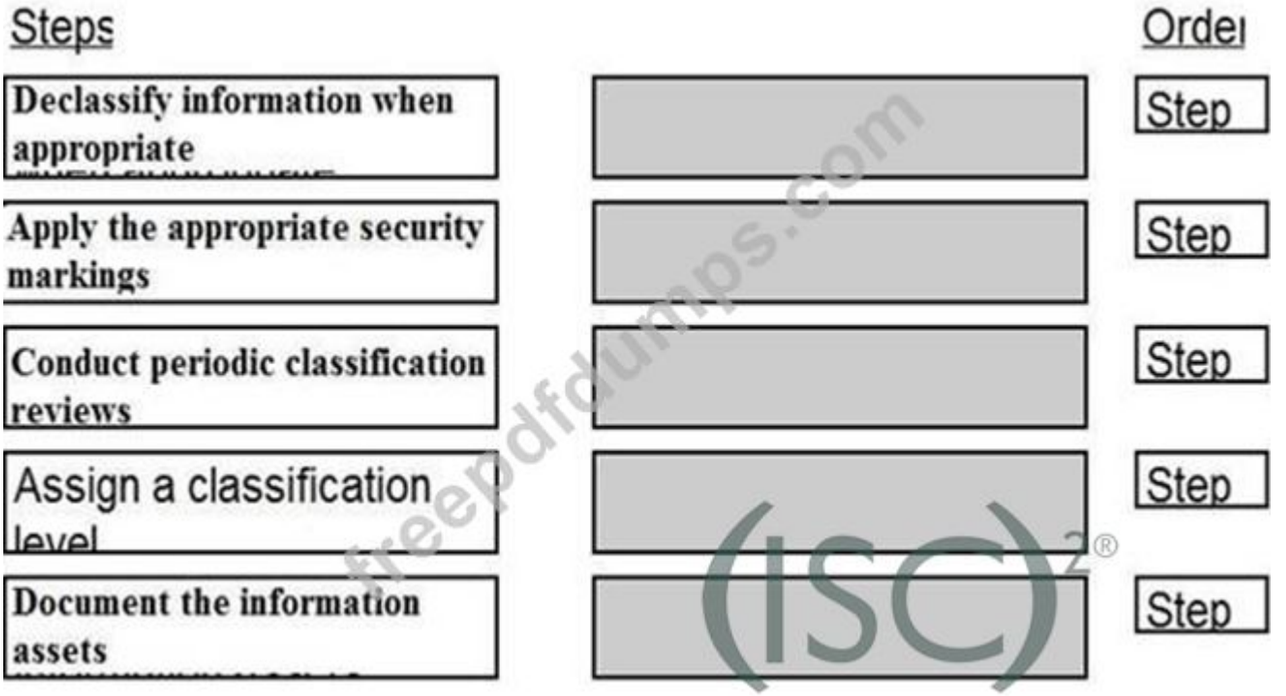
Access levels and permissions are audited to ensure they are in line with the user's current role and responsibilities.
Unnecessary access or permissions that go beyond what is required for the user's duties can be revoked.
This process ensures that employees are not granted more privileges than needed, helping to reduce the risk of accidental or malicious misuse of privileges.

NEW QUESTION: 113
確保無法檢索殘留資料的最有效的介質清理形式是什麼？
A. 清除
B. 摧毀
C. 清除
D. 處置
Answer: B (LEAVE A REPLY)
The most effective form of media sanitization to ensure residual data cannot be retrieved is destroying. Media sanitization is the process of removing or destroying the data stored on a physical or logical media, such as a hard drive, a flash drive, or a cloud storage, to prevent unauthorized access or disclosure. Destroying is the most extreme form of media sanitization, which involves the physical destruction of the media, such as shredding, crushing, melting, or incinerating. Destroying can ensure that the residual data cannot be retrieved by any means, as the media is rendered unusable and irreparable. Destroying is usually applied to the media that contains highly sensitive or classified data, or the media that is no longer needed or functional.

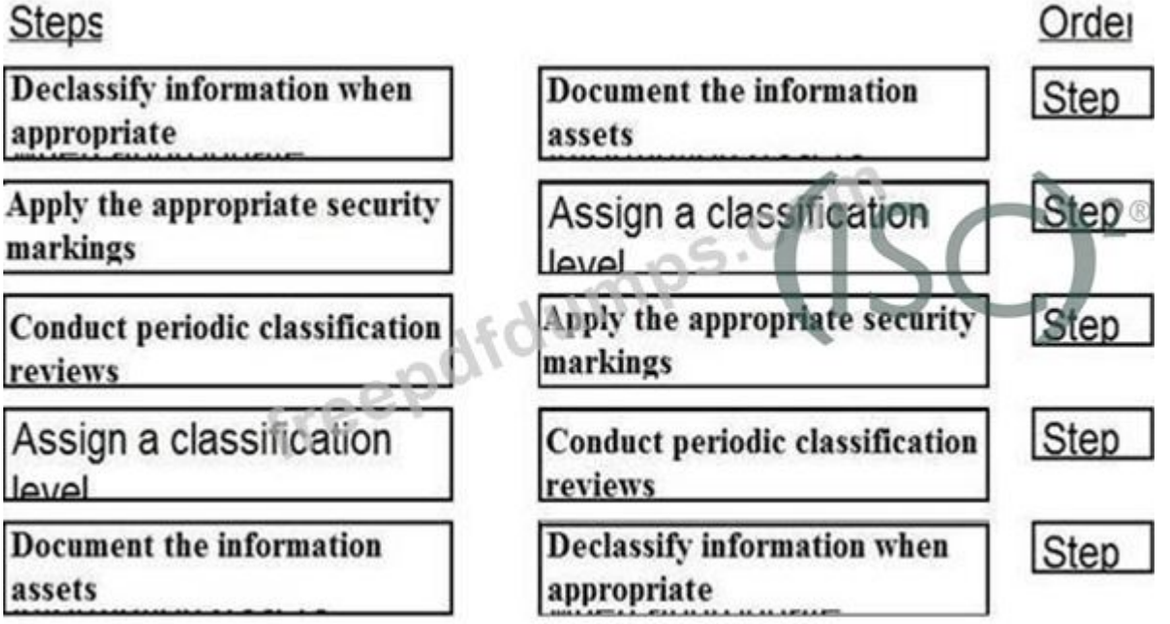
NEW QUESTION: 114
當安全管理員根據前兆和其他指標偵測到網路入侵時，首先應該採取什麼行動？
A. 隔離並遏制入侵。
B. 通知系統和應用程式擁有者。
C. 將修補程式套用至作業系統 (OS)。
D. 記錄並驗證入侵。
Answer: (SHOW ANSWER)
The first action for a security administrator who detects an intrusion on the network based on precursors and other indicators is to isolate and contain the intrusion. An intrusion is an unauthorized or malicious activity that attempts to compromise the security or the functionality of a system or a network. An intrusion can be detected by various methods, such as the analysis of the network traffic, the logs, the alerts, or the anomalies. Precursors and indicators are the signs or the evidence of an intrusion or an attempted intrusion. Precursors are the events or the activities that occur before or during an intrusion, such as the reconnaissance, the scanning, or the probing. Indicators are the events or the activities that occur after or as a result of an intrusion, such as the exploitation, the backdoor, or the payload. The first action for a security administrator who detects an intrusion on the network is to isolate and contain the intrusion, which means to disconnect or block the affected system or network from the rest of the environment and prevent the intrusion from spreading or causing more damage.

Isolating and containing the intrusion can help protect the other systems or networks from being compromised, preserve the evidence for the investigation, and facilitate the recovery and the restoration of the normal operations.

NEW QUESTION: 115
拖放題
請依序排列以下資訊分類步驟。



Answer:



NEW QUESTION: 116
法證專家如何將目標系統副本上的大部分作業系統檔案排除在檢口範圍之外？
A. 對相關媒體進行另一次備份，然後刪除所有無關的作業系統檔案

B. 建立來自具有相同作業系統和修補程式等級的系統的檔案的加密雜湊的比較資料庫。
C. 在磁碟機映像上□生訊息摘要 (MD) 或安全哈希，以偵測正在檢□的媒體是否已被竄改
D. 丟棄作業系統的無害檔案和已知已安裝程式。
Answer: B (LEAVE A REPLY)
A forensic specialist can exclude from examination a large percentage of operating system files residing on a copy of the target system by creating a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level. This method is also known as known file filtering or file signature analysis. It allows the forensic specialist to quickly identify and eliminate the files that are part of the standard operating system installation and focus on the files that are unique or relevant to the investigation. This makes the process of exclusion much faster and more accurate than manually deleting or discarding files.

NEW QUESTION: 117
以下哪□最能描述“出口点后量子密□迁移□划”的目的？
A. 立即用量子□算机替□所有□有的加密系□
B. 主□□点□□当前的加密使用情况，□□最易受未来量子攻□影响的系□，并在此□攻□□得切□可行之前制定分□段迁移到抗量子算法的□划。
C. □适用于已□有量子□算机的□□的□划流程
D. 一种□□用于提升当前□称加密性能的技□
Answer: B (LEAVE A REPLY)
Post-quantum cryptography migration planning involves proactively inventorying an organization's current cryptographic algorithm usage (particularly asymmetric algorithms like RSA and ECC that are most vulnerable to future quantum attacks), identifying and prioritizing the systems and data most at risk (especially long-lived sensitive data subject to "harvest now, decrypt later" attacks), and developing a phased migration plan to quantum-resistant algorithms well before large-scale, cryptographically relevant quantum computers become practical.

NEW QUESTION: 118
在電腦上進行法醫犯罪調□時，分析之前應該定義什麼？
A. 建立磁碟機上所有重要檔案的備份副本。
B. 關閉電腦電源並等待協助。
C. 建立硬碟的取證映像。
D. 安裝取證分析軟體。
Answer: C (LEAVE A REPLY)
When conducting a forensic criminal investigation on a computer hard drive, the first thing that should be done prior to analysis is to create a forensic image of the hard drive. A forensic image is a bit-by-bit copy of the original data source that preserves the integrity and authenticity of the evidence. A forensic image should be created using a write-blocker device or software that prevents any modification or alteration of the data on the hard drive. A forensic image should also be verified using a hash function that generates a unique value that can be used to validate the accuracy and completeness of the

image. A forensic image can then be analyzed using forensic analysis software or tools without affecting the original data source.

NEW QUESTION: 119
在軟體採購過程的下列哪個階段會制定評估標準？
A. 後續
B. 規劃
C. 承包
D. 監測與驗收
Answer: B (LEAVE A REPLY)
The software acquisition process is the process of acquiring software from external sources, such as vendors or contractors. It involves several phases, such as planning, contracting, monitoring and acceptance, and follow-on. Developing evaluation criteria is part of the planning phase, where the organization defines the requirements, objectives, and constraints of the software acquisition project. Evaluation criteria are the standards or measures that are used to assess the quality, suitability, and value of the software products or services offered by the potential suppliers. Developing evaluation criteria in the planning phase helps the organization to select the best software solution for its needs and goals.

NEW QUESTION: 120
哪种□□控制模型使用“机密”、“秘密”和“□密”等□□来□制□行□□决策？
A. 自主□□控制(DAC)
B. 基于角色的□□控制(RBAC)
C. □制□□控制(MAC)
D. 基于属性的□□控制(ABAC)
Answer: (SHOW ANSWER)
MAC enforces access based on security labels/classifications assigned to subjects and objects, with access decisions made by the system according to policy rather than by resource owners.
This is typical of military and government classification systems using labels like Confidential, Secret, and Top Secret.

NEW QUESTION: 121
客□已審□漏洞評估報告並表示該報告不準確。用□端指出列出的漏洞無效，因為未正確偵測到主機的作業系統 (OS)。
在漏洞評估過程中，錯誤最有可能發生在哪裡？
A. 列舉
B. 檢測
C. 報告
D. 發現
Answer: D (LEAVE A REPLY)

The error most likely occurred in the discovery phase of the vulnerability assessment process. Discovery is the phase where the assessor identifies the hosts, services, and applications that are present on the target network or system. Discovery can be done using active or passive methods, such as scanning, sniffing, or querying. If the discovery phase is not performed correctly, the assessor may miss some hosts or misidentify their operating systems, which can lead to inaccurate or incomplete results in the subsequent phases of the vulnerability assessment process.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 122
增強與關鍵系統互動的單一登入 (SSO) 解決方案的安全性的最有效方法是什麼？
A. 雙重認證
B. 用於應用程式層級驗證的可重複使用令牌
C. 高效能加密演算法
D. 用於所有通訊的安全通訊端層 (SSL)
Answer: A (LEAVE A REPLY)
Two-factor authentication (2FA) adds an additional layer of security to the authentication process by requiring users to provide two forms of identification: something they know (e.g., a password) and something they have (e.g., a physical token or a mobile device). This approach significantly reduces the risk of unauthorized access even if the user's password is compromised.

NEW QUESTION: 123
哪种密□攻□是指攻□者□取明文及其□□的密文□，从而推断出加密密□？
A. □密文攻□
B. 已知明文攻□
C. □□密文攻□
D. 生日□□
Answer: B (LEAVE A REPLY)
In a known-plaintext attack, the attacker has access to both plaintext and its corresponding ciphertext and attempts to derive the key or algorithm details. This differs from a ciphertext-only attack (only ciphertext available) and a chosen-ciphertext attack (attacker can choose ciphertext to decrypt).

NEW QUESTION: 124
以下哪□最能描述“出口点□私增□技□(PET)”(例如差分□私)的目的？
A. □了消除任何数据保□法□的必要性

B. 在数学上限制□□或推断数据集中任何特定个人信息的能力的同□，□□□数据的有效分析或共享。
C. □用于出于□管合□目的□数据□行加密
D. 一种□用于保□□□文件的技□
Answer: (SHOW ANSWER)
Privacy-Enhancing Technologies such as differential privacy introduce carefully calibrated statistical noise or other mathematical techniques into datasets or query results, enabling organizations to perform useful aggregate analysis or share data while providing strong, quantifiable guarantees that the presence or absence of any single individual's data cannot be reliably inferred, helping balance data utility with individual privacy protection.

NEW QUESTION: 125
如果調□人員想要分析可能用作證據的硬碟，最佳方法是什麼？
A. 請勿移動硬碟，並僅使用經過驗證和認證的作業系統(OS) 工具來分析其□容。
B. 登入系統並立即將所有相關檔案複製到一次寫入多次讀取 (WORM) 裝置。
C. 從系統中取出硬碟，並使用映像硬體複製硬碟的□容。
D. 在□動系統和分析硬碟之前，使用單獨的可□動裝置複製硬碟。
Answer: (SHOW ANSWER)
When handling a hard drive that may be used as evidence in an investigation, the best practice is to remove the hard drive from the system and then create an exact forensic image of the drive using imaging hardware or forensic software. This process ensures that the original evidence is not altered or damaged during the investigation.
Creating a forensic image of the drive is a critical step in preserving the integrity of the evidence.
The forensic image is a bit-by-bit copy of the entire drive, including hidden files, deleted data, and unallocated space, ensuring that no evidence is lost or corrupted. This also allows the investigator to work with a copy of the data, leaving the original hard drive unchanged and maintaining the chain of custody.

NEW QUESTION: 126
以下哪□最能描述“出口点数据保□影响□估(DPIA)”的目的？
A. □□□数据存□成本的□□□□
B. 一种□构化流程，用于□□和降低与涉及个人数据□理的新□目 系□或流程相关的□私□□，通常是 GDPR 等法□□□高□□□理活□所要求的。
C. 一□□□□□网□基□□施的技□渗透□□
D. □在□生数据泄露后使用的流程
Answer: B (LEAVE A REPLY)
A Data Protection Impact Assessment is a structured, proactive process used to identify, assess, and mitigate privacy risks associated with a new project, system, or process that involves processing personal data-particularly for high-risk processing activities-often mandated under privacy regulations such as GDPR before the processing activity begins, rather than as a reactive measure following an incident.

NEW QUESTION: 127
已確定並認定某些人員有必要知悉該資訊。
下列哪些存取控制方法必須包含一套一致的規則來控制和限制存取？
A. 基於屬性的存取控制(ABAC)
B. 基於角色的存取控制(RBAC)
C. 自主存取控制(DAC)
D. 強制存取控制(MAC)
Answer: B (LEAVE A REPLY)
Role-Based Access Control (RBAC) is an access control method that assigns permissions to users based on their roles or functions within an organization. RBAC requires a consistent set of rules for controlling and limiting access, as each role is defined by a set of access rights that correspond to the level of authority and responsibility of the role. RBAC can simplify access management, enforce the principle of least privilege, improve security and compliance, and reduce administrative overhead.

NEW QUESTION: 128
公司□部已簽署並實施了涵蓋安全性方面的服務等級協定 (SLA)。為了確保良好的安全態勢得以實現，何時應該審□ SLA 的遵守情況？
A. 作為 SLA 續約流程的一部分
B. 在計劃的安全審計之前
C. 安全漏洞發生後立即
D. 在定期會議上
Answer: (SHOW ANSWER)
Compliance to the SLA should be reviewed at regularly scheduled meetings, such as monthly or quarterly, to ensure that the security posture is being delivered as agreed. This allows both parties to monitor the performance, identify any issues or gaps, and take corrective actions if needed. Reviewing the SLA only as part of the renewal process, prior to a planned security audit, or immediately after a security breach is not sufficient, as it may result in missing or delaying the detection and resolution of security problems.

NEW QUESTION: 129
某個組織正在考慮將應用程式和資料外包給雲端服務供應商 (CSP)。下列哪一項是有關隱私的最重要問題？
A. CSP 確定資料的關鍵性。
B. CSP 提供端對端加密服務。
C. CSP 的隱私權政策可以由組織制定。
D. CSP 可能不受該組織所在國家的委託。
Answer: D (LEAVE A REPLY)
Privacy is the right or ability of individuals or groups to control or limit the collection, use, disclosure, or retention of their personal or sensitive data by others. Privacy is an important concern for organizations

that are considering outsourcing applications and data to a Cloud Service Provider (CSP). The most important concern regarding privacy is that the CSP may not be subject to the organization's country legislation. The organization's country legislation may have specific laws, regulations, or standards that govern the privacy of data, such as the General Data Protection Regulation (GDPR) in the European Union, or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. However, the CSP may operate in a different country or jurisdiction that has different or less stringent privacy laws, regulations, or standards.
This may create a conflict or a gap between the organization's privacy obligations and the CSP's privacy practices, and expose the organization to legal, regulatory, or reputational risks.
Therefore, the organization should carefully review the CSP's privacy policy and contract, and ensure that the CSP complies with the organization's country legislation and the organization's privacy requirements and expectations. The CSP determining data criticality, providing end-to- end encryption services, or allowing the organization to develop its privacy policy are not the most important concerns regarding privacy, as they are more related to data security, data protection, or data governance.

NEW QUESTION: 130
一家組織開發了一種讓客口彼此分享穿戴式裝置資訊的方法。不幸的是，用口沒有被告知所收集的哪些資訊將被分享。應採取哪些技術控制措施來解決隱私問題，同時仍努力實現組織的業務目標？
A. 預設使用者不分享任何資訊。
B. 通知使用者分享功能實施後的變更。
C. 只分享組織認為最好的口容。
D. 停止與其他使用者分享資料。
Answer: A (LEAVE A REPLY)
The privacy issue in this scenario is that the users were not informed as to what information collected would be shared with other users, and they did not give their consent to share their information. This violates the privacy principles of notice and choice, which state that the users should be notified of the data collection and sharing practices of the organization, and they should be given the option to opt-in or opt-out of the sharing feature. The technical control that should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals is to default the user to not share any information, and to provide the user with a clear and easy way to enable the sharing feature if they wish to do so. This way, the user's privacy is respected and protected, and the user can still participate in the sharing feature if they find it beneficial. The other answer choices are not appropriate, because they either do not address the privacy issue, or they do not support the organization's business goals.

NEW QUESTION: 131
雲端服務提供者要求其客口組織為其資料儲存服務口用最大程度的審核日誌記錄，並將日誌保留三個月。審核日誌記錄會口生大量日誌。日誌保留最適合的策略是什麼？
A. 將上週的日誌保存在線上儲存中，其餘日誌保存在近線儲存中。
B. 將所有日誌保存在線上儲存中。
C. 將所有日誌保存在離線儲存中。

D. 將上週的日誌保存在線上儲存中，其餘日誌保存在離線儲存中。

Answer: (SHOW ANSWER)

The most appropriate strategy for the log retention of a cloud service provider that requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months, given that the audit logging generates extremely high amount of logs, is to keep last week's logs in an online storage and the rest in a near-line storage.

Online storage is a type of storage that is directly accessible by the system or application, such as hard disk drives, solid state drives, or flash drives. Online storage is fast, convenient, and reliable, but it is also expensive and consumes more power. Near-line storage is a type of storage that is not directly accessible by the system or application, but can be made accessible within a short time, such as tape drives, optical disks, or removable media. Near-line storage is slower, less convenient, and less reliable than online storage, but it is also cheaper and consumes less power. By keeping last week's logs in an online storage and the rest in a near-line storage, the cloud service provider can balance the trade-offs between performance, cost, and availability of the logs. The logs that are most likely to be accessed or analyzed are kept in the online storage, while the logs that are less likely to be accessed or analyzed are kept in the near-line storage.

This way, the cloud service provider can meet the log retention requirement without wasting too much resources or compromising the security of the logs. Keeping all logs in an online storage, keeping all logs in an offline storage, or keeping last week's logs in an online storage and the rest in an offline storage are not appropriate strategies for the log retention of the cloud service provider. Keeping all logs in an online storage would be too costly and inefficient, as it would consume too much disk space and power for logs that are rarely accessed or analyzed. Keeping all logs in an offline storage or keeping last week's logs in an online storage and the rest in an offline storage would be too risky and inconvenient, as it would make the logs inaccessible or difficult to access in case of an audit, investigation, or incident response. Offline storage is a type of storage that is not accessible by the system or application, and requires manual intervention to access, such as archived tapes, disks, or media.

NEW QUESTION: 132

一家成熟的資訊科技(IT)顧問公司正在考慮收購一家成功的本地新創公司。為了全面了解這家新創公司的安全狀況，哪種評估方法能提供最佳資訊？

A. 安全審計

B. 滲透測試

C. 桌面演練

D. 安全威脅模型

Answer: B (LEAVE A REPLY)

A penetration test is the best type of assessment to gain a comprehensive understanding of the startup's security posture. A penetration test is a simulated attack on a system or a network, performed by authorized testers, to evaluate the security and vulnerability of the system or network. A penetration test can provide the following benefits for the IT consulting firm that is considering acquiring the startup:

It can reveal the actual risks and impacts of the potential attacks or threats on the system or network, by exploiting the vulnerabilities or weaknesses in the system or network.
It can measure the effectiveness and maturity of the security controls and policies implemented by the system or network, by testing the detection, prevention, and response capabilities of the system or network.
It can provide the recommendations and solutions for improving the security and resilience of the system or network, by identifying and prioritizing the remediation actions for the system or network. A penetration test can provide more comprehensive and realistic information about the startup's security posture than other types of assessments, such as a security audit, a tabletop exercise, or a security threat model, which are more theoretical, formal, or hypothetical in nature.

NEW QUESTION: 133
在電腦系統外殼上放置防口改密封件的主要目的是：
A. 提高安全意識。
B. 檢測打開案件的努力。
C. 加快物理審核。
D. 使口部元件難以被竊取。
Answer: B (LEAVE A REPLY)
A tamper seal is a device or material that is attached to a computer system's case to indicate whether the case has been opened or tampered with. The main purpose of placing a tamper seal on a computer system's case is to detect efforts to open the case, as the seal will be broken or damaged if someone tries to access the internal components of the system. This can help deter unauthorized access, prevent physical damage or theft, and provide evidence for forensic investigation. Raising security awareness is not the main purpose of placing a tamper seal on a computer system's case, although it may have a secondary effect of reminding users of the importance of physical security. Expediting physical auditing is not the main purpose of placing a tamper seal on a computer system's case, although it may have a secondary effect of simplifying the process of checking the integrity of the system. Making it difficult to steal internal components is not the main purpose of placing a tamper seal on a computer system's case, although it may have a secondary effect of increasing the effort and risk of the attacker.

NEW QUESTION: 134
考慮到組織的系統不能超過 24 小時不可用，災難復原(DR) 站點最具成本效益的解決方案是什麼？
A. 溫暖站點
B. 熱門站點
C. 鏡像站點
D. 冷站點
Answer: A (LEAVE A REPLY)
A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours. A DR site is a backup facility that can be used to restore the normal operation of the organization's IT systems and infrastructure after a

disruption or disaster. A DR site can have different levels of readiness and functionality, depending on the organization's recovery objectives and budget. The main types of DR sites are:
Hot site: a DR site that is fully operational and equipped with the necessary hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running almost immediately. A hot site has all the required servers, workstations, and communications links, and can function as a branch office or data center that is online and connected to the production network. A hot site also has a backup of the data from the systems at the primary site, which may be replicated in real time or near real time. A hot site greatly reduces or eliminates downtime for the organization, but it is also very expensive to maintain and operate.
Warm site: a DR site that is partially operational and equipped with some of the hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running within a short time. A warm site has some of the required servers, workstations, and communications links, and can function as a temporary office or data center that is offline or partially connected to the production network. A warm site may have a backup of the data from the systems at the primary site, but it is not updated or synchronized as frequently as a hot site. A warm site reduces downtime for the organization, but it is also less expensive than a hot site.
Cold site: a DR site that is not operational and equipped with only the basic infrastructure and environmental support systems to allow the organization to be up and running within a long time.
A cold site has none of the required servers, workstations, and communications links, and cannot function as an office or data center until they are installed and configured. A cold site does not have a backup of the data from the systems at the primary site, and it has to be restored from other sources, such as tapes or disks. A cold site increases downtime for the organization, but it is also the cheapest option among the DR sites.
Mirror site: a DR site that is an exact replica of the primary site, with the same hardware, software, telecommunication lines, and network connectivity, and with the same data and applications. A mirror site is always online and synchronized with the primary site, and can take over the operation of the organization seamlessly in the event of a disruption or disaster. A mirror site eliminates downtime for the organization, but it is also the most expensive option among the DR sites.
A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it can provide a balance between the recovery time and the recovery cost. A warm site can enable the organization to resume its critical functions and operations within a reasonable time frame, without spending too much on the DR site maintenance and operation. A warm site can also provide some flexibility and scalability for the organization to adjust its recovery strategies and resources according to its needs and priorities.

NEW QUESTION: 135
由於建立的密鑰數量眾多，下列哪一項是最重要的密鑰管理問題？
A. 金鑰更難配置且
B. 金鑰的儲存需要提高安全性
C. 使用非對稱金鑰時呈指數成長
D. 使用對稱金鑰時呈指數成長

Answer: D (LEAVE A REPLY)

Key management is the process of generating, distributing, storing, using, and destroying cryptographic keys. One of the most significant key management problems is the number of keys created, which affects the complexity, scalability, and security of the cryptographic system. The number of keys created depends on the type of encryption used: symmetric or asymmetric.

Symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. When using symmetric encryption, the number of keys created grows exponentially with the number of users or devices involved. For example, if there are n users or devices that need to communicate securely with each other, then each user or device needs to have a unique key for each other user or device. Therefore, the total number of keys needed is n(n-1)/2, which is an exponential function of n. This means that as the number of users or devices increases, the number of keys needed increases dramatically, making it more difficult to provision, store, and protect the keys.

When using asymmetric encryption, the number of keys created grows linearly with the number of users or devices involved. For example, if there are n users or devices that need to communicate securely with each other, then each user or device needs to have only one pair of keys: a public key and a private key. Therefore, the total number of keys needed is 2n, which is a linear function of n. This means that as the number of users or devices increases, the number of keys needed increases proportionally, making it easier to provision, store, and protect the keys.

NEW QUESTION: 136

對於使用公有雲服務的組織來口，下列哪一種媒體清理技術最有可能有效？

A. 低階格式化

B. 安全級覆蓋擦除

C. 加密擦除

D. 驅動消磁

Answer: (SHOW ANSWER)

Media sanitization is the process of rendering the data on a storage device inaccessible or unrecoverable by a given level of effort. For an organization using public cloud services, the most effective media sanitization technique is cryptographic erasure, which involves encrypting the data on the device with a strong key and then deleting the key, making the data unreadable.

Cryptographic erasure is suitable for cloud environments because it does not require physical access to the device, it can be performed remotely and quickly, and it does not affect the performance or lifespan of the device. Low-level formatting, secure-grade overwrite erasure, and drive degaussing are media sanitization techniques that require physical access to the device, which may not be possible or feasible for cloud users. Additionally, these techniques may not be compatible with some cloud storage technologies, such as solid-state drives (SSDs) or flash memory, and they may reduce the performance or lifespan of the device.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 137
下列哪一項需要識別到業務流程、應用程式和資料儲存的資料端連結以及所有權責任的分配？
A. 風險管理
B. 安全組合管理
C. 安全治理
D. 風險評估
Answer: B (LEAVE A REPLY)
Security portfolio management is the process of identifying, classifying, and managing the data assets of an organization, as well as assigning ownership responsibilities and defining protection requirements. Security portfolio management entails identification of data and links to business processes, applications, and data stores, as well as assessment of data value, sensitivity, and risk. Security portfolio management can help an organization achieve data security, compliance, and governance objectives.

NEW QUESTION: 138
實施數位簽章時存在下列哪些威脅？
A. 欺騙
B. 替換
C. 口容竄改
D. 竊聽
Answer: B (LEAVE A REPLY)
Substitution is a threat that occurs when an attacker replaces a valid digital signature with an invalid one, or a signature from another document. This can compromise the integrity and non- repudiation of the signed document, as the receiver cannot verify the authenticity and origin of the document. Substitution can be prevented by using secure hash algorithms and encryption to generate and protect the digital signatures.

NEW QUESTION: 139
在口動軟體開發時，解決潛在的安全性問題根本上需要下列哪一項？
A. 在所有環境中實施持續的安全審核。
B. 確保開發與生口的隔離。
C. 將資訊安全目標加入開發。
D. 進行獨立的原始碼審口。
Answer: C (LEAVE A REPLY)

The fundamental requirement to address potential security issues when initiating software development is to add information security objectives into development. This means that security should be considered as an integral part of the software development life cycle (SDLC), from the initial planning and analysis phase to the final deployment and maintenance phase. Security objectives should be aligned with the business objectives and requirements of the software, and should be measurable, achievable, and verifiable. Security objectives should also be communicated and agreed upon by all the stakeholders involved in the software development, such as developers, testers, users, and managers. Adding security objectives into development can help to prevent, detect, and mitigate security flaws and vulnerabilities in the software, and to ensure that the software meets the security standards and expectations of the organization and the customers.

NEW QUESTION: 140
由於電話供應商的費用大幅上漲，安全工程師正在對組織的網際網路協定語音(VoIP) 電話網路進行審核。工程師發現未經授權的端點已從公共互聯網連接到電話伺服器，並向全球各地的各方發出了數百個未經授權的呼叫。發生了哪種類型的攻擊？
A. 話費欺詐
B. 地址欺騙
C. 呼叫劫持
D. 控制竊聽
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
下列哪項漏洞評估活動最能反映檢口評估方法？
A. 確保系統審核日誌擷取安全控制基線所需的所有相關資料字段
B. 對選定的網路主機執行連接埠掃描以列舉活動服務
C. 要求資訊系統安全官 (ISSO) 描述組織的修補程式管理流程
D. 使用預設管理員帳口和預設密碼登入網頁伺服器
Answer: C (LEAVE A REPLY)
Asking the Information System Security Officer (ISSO) to describe the organization's patch management processes is the vulnerability assessment activity that best exemplifies the Examine method of assessment. The Examine method of assessment is a type of vulnerability assessment method that involves reviewing and analyzing the documentation, policies, procedures, and configurations of the system or network, to identify any gaps, weaknesses, or inconsistencies that may pose a security risk. The Examine method of assessment does not involve any active testing or scanning of the system or network, but rather relies on the information and evidence provided by the system or network owners, administrators, or users. Asking the ISSO to describe the organization's patch management processes is an example of the Examine method of assessment, as it involves reviewing and analyzing the patch management policies and procedures, to determine if they are adequate, effective, and compliant with the security standards and best practices.

NEW QUESTION: 142

敏感資訊的資料外洩最常透過以下哪種方式掩蓋？
A. 安全通訊端層 (SSL)
B. 安全雜湊演算法(SHA)
C. 有線等效加密 (WEP)
D. 安全郵局協定(POP)
Answer: (SHOW ANSWER)
Data leakage of sensitive information is most often concealed by Secure Sockets Layer (SSL), which is a protocol that provides encryption and authentication for data transmitted over a network. SSL can prevent eavesdropping, tampering, and spoofing of data by encrypting the data with a symmetric key and verifying the identity of the parties with a digital certificate. SSL can also provide data integrity by using a message authentication code (MAC) to detect any alteration of the data. SSL is widely used for securing web traffic, email, instant messaging, and other applications that require confidentiality and integrity of data

NEW QUESTION: 143
下列哪一項是最強的實體存取控制？
A. 生物辨識與徽章讀取器
B. 生物辨識、密碼與個人識別碼 (PIN)
C. 每個使用者的單獨密碼
D. 生物辨識、密碼和徽章讀取器
Answer: (SHOW ANSWER)
The strongest physical access control is the combination of biometrics, a password, and a badge reader. A physical access control is a security mechanism that restricts and regulates the access to a physical location, such as a building, a room, or a device. A physical access control can use different types of authentication factors, such as something the user knows (e.g., a password or a PIN), something the user has (e.g., a badge or a token), or something the user is (e.g., a fingerprint or a face). The combination of biometrics, a password, and a badge reader is the strongest physical access control, as it requires the user to present three different and independent authentication factors, which increases the security and reduces the likelihood of unauthorized access. This type of physical access control is also known as multi-factor authentication or MFA.

NEW QUESTION: 144
在解決道德衝突時，資訊安全專業人員必須考慮許多因素 這些考慮因素應該以什麼順序排列？
A. 公共安全、對個人的責任、對職業的責任和對校長的責任
B. 公共安全、對校長的責任、對個人的責任和對職業的責任
C. 公共安全、對職業的責任、對校長的責任和對個人的責任
D. 公共安全、對校長的責任、對職業的責任和對個人的責任
Answer: A (LEAVE A REPLY)
The order in which the information security professional must consider the factors when resolving ethical conflicts is public safety, duties to individuals, duties to the profession, and duties to principals.

Ethics are the principles or standards that guide the conduct or behavior of a person or a group. Ethics are important for the information security profession, as the information security professionals have the responsibility to protect the confidentiality, integrity, and availability of the information and systems they manage or access, and to ensure the trust and confidence of the stakeholders and the society. The information security professionals may face ethical conflicts or dilemmas, which are situations where there are two or more choices that have different ethical implications or consequences, and no clear or easy solution. When resolving ethical conflicts, the information security professional must consider the following factors, in the order of priority:
Public safety: The information security professional must protect the health, safety, and welfare of the public, and avoid any actions or decisions that could harm or endanger the public.
Duties to individuals: The information security professional must respect the rights, privacy, and dignity of the individuals, and avoid any actions or decisions that could harm or discriminate the individuals.
Duties to the profession: The information security professional must uphold the reputation, integrity, and competence of the profession, and follow the code of ethics and standards of practice of the profession.
Duties to principals: The information security professional must act in the best interest of the principals, such as the employers, clients, or customers, and fulfill the contractual obligations and fiduciary duties to the principals.

NEW QUESTION: 145
下列哪些方法可以用來確保傳輸中資料的機密性和完整性？
A. 多重協定標籤交換(MPLS)
B. 網際網路協定安全(IPSec)
C. 聯邦身分管理
D. 多因素身份驗證
Answer: B (LEAVE A REPLY)
IPSec provides confidentiality and integrity for data in transit by encrypting and authenticating all IP packets exchanged between participating devices.

NEW QUESTION: 146
下列哪一項是點對點協定 (PPP) 的對等實體驗證方法？
A. 質詢握手驗證協定 (CHAP)
B. 訊息驗證碼 (MAC)
C. 傳輸層安全性 (TLS) 握手協定
D. 挑戰回應認證機制
Answer: A (LEAVE A REPLY)
Point-to-Point Protocol (PPP) is a network protocol that provides a simple and secure way of establishing a direct connection between two hosts over a serial link, such as a phone line or a cable. PPP supports various methods of peer entity authentication, which is the process of verifying the identity and credential of the hosts involved in the connection. One of the peer entity authentication methods supported by PPP is Challenge Handshake Authentication Protocol (CHAP). CHAP is a

challenge-response authentication mechanism that uses a shared secret, such as a password, and a one-way hash function, such as MD5, to authenticate the hosts.
CHAP periodically sends a random challenge to the host, and the host responds with a hash of the challenge and the secret. The challenger then compares the hash with its own calculation and accepts or rejects the host. CHAP provides a secure and efficient way of authenticating the hosts without sending the secret over the network. Message Authentication Code (MAC), Transport Layer Security (TLS) handshake protocol, or challenge-response authentication mechanism are not peer entity authentication methods for PPP, as they are more related to data integrity, secure communication, or general authentication concepts.

NEW QUESTION: 147
以下哪□最能描述“出口点□□透明度 (CT)”日志的用途？
A. □□□□□机构提供一个私密、加密的通道来□□□□。
B. 提供一个公开的、□可追加的已□□ TLS □□□□，使域名所有者和研究人□能□□□□定域名的未□授□或□□□□的□□。
C. 自□撤□□期□□
D. 用于管理□□□□机构的私□存□
Answer: B (LEAVE A REPLY)
Certificate Transparency logs provide a public, cryptographically verifiable, append-only record of all TLS certificates issued by participating certificate authorities, allowing domain owners, browsers, and researchers to monitor for and detect unauthorized, mis-issued, or fraudulently obtained certificates for a given domain, improving overall trust in the PKI ecosystem.

NEW QUESTION: 148
一個化學計劃想要升級工業控制系統 (ICS)，以使用乙太網路而不是RS422 傳輸資料。專案經理希望透過利用辦公室網路基礎設施和人員來實施本次升級，從而簡化管理和維護。
下列哪一項對網路安全影響最大？
A. 網路管理員不了解ICS
B. 現在可以從辦公室網路存取 ICS
C. ICS 不支援 Office 密碼原則
D. RS422 比乙太網路可靠
Answer: B (LEAVE A REPLY)
The greatest impact on security for the network is that the ICS is now accessible from the office network. This means that the ICS is exposed to more potential threats and vulnerabilities from the internet and the office network, such as malware, unauthorized access, data leakage, or denial- of-service attacks. The ICS may also have different security requirements and standards than the office network, such as availability, reliability, and safety. Therefore, connecting the ICS to the office network increases the risk of compromising the confidentiality, integrity, and availability of the ICS and the critical infrastructure it controls.

NEW QUESTION: 149
使用強身份驗證、對資料庫伺服器上的個人識別資訊 (PII) 進行加密、進行應用程式安全審口以及對透過網路傳輸的資料進行加密，可以提供安全保障
A. 資料完整性。
B. 縱深防禦。
C. 數據可用性。
D. 不可否認性。
Answer: B (LEAVE A REPLY)
Defense in depth is a security strategy that involves applying multiple layers of protection to a system or network to prevent or mitigate attacks. The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks are examples of defense in depth measures that can enhance the security of the system or network.

NEW QUESTION: 150
下列哪一項是實施企業身分和存取管理 (IAM) 解決方案的好處？
A. 簡化了密碼要求。
B. 與孤兒帳口相關的風險降低。
C. 自動強制執行職責分離。
D. 提高資料機密性。
Answer: B (LEAVE A REPLY)
An enterprise Identity and Access Management (IAM) solution is designed to centralize and streamline the management of user identities and their access to systems, applications, and data.
One of the key benefits of implementing IAM is that it helps reduce the risk associated with orphan accounts.
Orphan accounts refer to user accounts that are still active but no longer associated with an active user (e.g., due to employee departures or role changes). These accounts can pose a significant security risk, as they often have elevated access and are typically forgotten, leaving them vulnerable to exploitation.
With an IAM solution, user accounts are tightly integrated with HR systems and business processes, ensuring that when an employee leaves or changes roles, their access is automatically revoked or updated. This reduces the chance that orphan accounts will persist and remain a potential security risk.

NEW QUESTION: 151
限制行動程式碼的處理器、記憶體和輸入/輸出 (I/O) 能力稱為
A. 代碼限制。
B. 按需編譯。
C. 沙箱。
D. 劃分。
Answer: C (LEAVE A REPLY)

Mobile code is a term that refers to any code that can be transferred from one system to another and executed on the target system, such as Java applets, ActiveX controls, or JavaScript scripts. Limiting the processor, memory, and input/output (I/O) capabilities of mobile code is known as sandboxing. Sandboxing is a security technique that isolates the mobile code from the rest of the system and restricts its access to the system resources, such as files, network, or registry. Sandboxing can prevent the mobile code from causing harm or damage to the system, such as installing malware, stealing data, or modifying settings.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 152
下列哪個流程的主要目的是識別過時的軟體版本、缺少的修補程式和失效的系統更新？
A. 滲透測試
B. 漏洞管理
C. 軟體開發生命週期 (SDLC)
D. 生命週期管理
Answer: B (LEAVE A REPLY)
Vulnerability management is the process that has the primary purpose of identifying outdated software versions, missing patches, and lapsed system updates. Vulnerability management is a systematic and proactive approach to identifying, assessing, and mitigating the vulnerabilities that may affect the organization's information systems and assets. A vulnerability is a weakness or a flaw in a system or an application that can be exploited by an attacker to compromise the security or the functionality of the system or the application. Vulnerability management can help prevent or reduce the impact of the attacks that may exploit the vulnerabilities, and improve the security and the quality of the information systems and assets. Vulnerability management has the primary purpose of identifying outdated software versions, missing patches, and lapsed system updates, as these are some of the common sources and causes of vulnerabilities. Outdated software versions, missing patches, and lapsed system updates can expose the system or the application to known or unknown vulnerabilities, such as bugs, errors, or security flaws, that can be exploited by the attackers. Vulnerability management can help identify these issues and resolve them by applying the latest software versions, patches, and updates, and by ensuring that the system or the application is up to date and secure.

NEW QUESTION: 153
下列哪一項是轉置密碼易於辨識的原因？
A. 按鍵

B. 阻止
C. 流
D. 字符
Answer: D (LEAVE A REPLY)
The reason that transposition ciphers are easily recognizable is character. A transposition cipher is a type of cipher that rearranges or permutes the order or position of the characters or symbols in the plaintext, without changing or altering the characters or symbols themselves, to produce the ciphertext. A transposition cipher can help to conceal the meaning or content of the plaintext, by making it difficult or impossible to read or understand the ciphertext, without knowing the key or algorithm that was used to transpose the characters or symbols. However, a transposition cipher is also easily recognizable, as it does not change or alter the frequency or distribution of the characters or symbols in the plaintext, which can be used to identify or analyze the ciphertext.
The reason that transposition ciphers are easily recognizable is character, which is the smallest unit or element of the plaintext or ciphertext, such as a letter, number, or symbol. Character is the reason that transposition ciphers are easily recognizable, as it is the basis or criterion for the transposition or permutation of the plaintext or ciphertext, as well as for the frequency or distribution analysis of the plaintext or ciphertext. Key, block, or stream are not the reasons that transposition ciphers are easily recognizable, as they are either more related to the encryption or decryption process, rather than the recognition or identification process, or to the other types of ciphers, such as substitution ciphers, which change or alter the characters or symbols in the plaintext, rather than rearrange or permute them.

NEW QUESTION: 154
使用者需要存取權限才能□看員工群組的平均薪資。
哪種控制會阻止使用者獲得單一員工的薪資？
A. 限制對預定義□詢的訪問
B. 將資料庫分成少量分割區，每個分割區具有單獨的安全級別
C. 實施基於角色的存取控制 (RBAC)
D. 為統計目的減少有權存取系統的人數
Answer: A (LEAVE A REPLY)
Limiting access to predefined queries is the control that would prevent the users from obtaining an individual employee's salary, if they only require access rights that allow them to view the average salary of groups of employees. A query is a request for information from a database, which can be expressed in a structured query language (SQL) or a graphical user interface (GUI).
A query can specify the criteria, conditions, and operations for selecting, filtering, sorting, grouping, and aggregating the data from the database. A predefined query is a query that has been created and stored in advance by the database administrator or the data owner, and that can be executed by the authorized users without any modification. A predefined query can provide several benefits, such as: Improving the performance and efficiency of the database by reducing the processing time and resources required for executing the queries Enhancing the security and confidentiality of the database by restricting the access and exposure of the sensitive data to the authorized users and purposes Increasing the accuracy and reliability of the database by preventing the errors or inconsistencies that

might occur due to the user input or modification of the queries Reducing the cost and complexity of the database by simplifying the query design and management Limiting access to predefined queries is the control that would prevent the users from obtaining an individual employee's salary, if they only require access rights that allow them to view the average salary of groups of employees, because it can ensure that the users can only access the data that is relevant and necessary for their tasks, and that they cannot access or manipulate the data that is beyond their scope or authority. For example, a predefined query can be created and stored that calculates and displays the average salary of groups of employees based on certain criteria, such as department, position, or experience. The users who need to view this information can execute this predefined query, but they cannot modify it or create their own queries that might reveal the individual employee's salary or other sensitive data.

NEW QUESTION: 155
下列哪一項敘述最能描述雲端環境中的最小特權原則？
A. 如果不需要存取互聯網，網段將保持私有。
B. 檢口網路流量中的所有傳入和傳出資料包。
C. 設定單一雲端管理員來存取核心功能。
D. 路由配置定期更新為最新路由。
Answer: C (LEAVE A REPLY)
The least privilege principle means that users, applications, or systems should only be given the minimum level of access required to perform their specific tasks, reducing the risk of unauthorized actions and minimizing the attack surface.
In the context of cloud environments:
C describes a scenario where only a single administrator has the necessary access to core functions (which follows the least privilege principle by limiting who can access critical resources).

NEW QUESTION: 156
在對資訊進行分類並支援風險管理、法律發現和合規性資口時必須考慮哪些因素？
A. 系統擁有者角色和職責、資料處理標準、儲存和安全開發生命週期要求
B. 資料管理角色、資料處理與儲存標準、資料生命週期需求
C. 合規辦公室角色與職責、分類物料搬運標準、儲存系統生命週期要求
D. 系統授權角色與職責、雲端運算標準、生命週期要求
Answer: B (LEAVE A REPLY)
When classifying information and supporting assets for risk management, legal discovery, and compliance, the key factors to consider are:
1. Data stewardship roles: This involves defining who is responsible for overseeing data throughout its lifecycle, including its classification, protection, and management. Data stewards ensure that data is handled appropriately according to internal policies, legal requirements, and compliance regulations.
2. Data handling and storage standards: Organizations need to establish standards for how data is handled (e.g., collection, access, sharing) and stored (e.g., encryption, storage methods).
These standards ensure that data is protected according to regulatory and organizational requirements.

3. Data lifecycle requirements: This refers to the need to manage data across its entire lifecycle- from creation and storage to deletion or archival. Properly managing the data lifecycle is essential for ensuring compliance, mitigating risks, and enabling legal discovery when necessary.

NEW QUESTION: 157
在設計網路實體系統(CPS)時，安全從業人員應該先考慮下列哪一項？
A. 系統的彈性
B. 偵測複雜攻擊者
C. 系統風險評估
D. 系統所用網路的拓樸結構
Answer: C (LEAVE A REPLY)
A Cyber-Physical System (CPS) is a system that integrates physical processes, computational capabilities, and communication networks. A CPS can have various applications, such as smart grids, autonomous vehicles, or industrial control systems. When designing a CPS, the first consideration for a security practitioner should be the risk assessment of the system, which is the process of identifying, analyzing, and evaluating the potential threats, vulnerabilities, and impacts that could affect the system. A risk assessment can help to determine the security requirements, objectives, and controls for the CPS, as well as the priorities and resources for the security implementation and management. Resiliency, detection, and topology are all important aspects of CPS security, but they are not the first consideration, as they depend on the outcome of the risk assessment.

NEW QUESTION: 158
下列哪一項是實作第三方聯合身分架構最顯著的好處？
A. 屬性斷言，因為機構可以要求更大的屬性集來完成服務交付
B. 與儲存個人資訊相關的資料減少
C. 降低機構的營運成本
D. 達成業務目標，以便各部門可以專注於任務而非身分管理業務
Answer: D (LEAVE A REPLY)
A third-party federated identity architecture is a system that allows users to access multiple services or applications across different domains or organizations using a single identity. The most significant benefit of implementing such an architecture is that it enables business objectives so departments can focus on their mission rather than the business of identity management. By delegating the authentication and authorization processes to a trusted third party, the departments can reduce the complexity, cost, and risk of managing their own identity systems, and improve the user experience and satisfaction.

NEW QUESTION: 159
如果懷疑病毒感染，使用者首先要採取下列哪一項措施？
A. 將電腦從網路上拔下。
B. 儲存開口的檔案並關閉電腦。
C. 向服務台報告事件。

D. 將防毒軟體更新至最新版本。

Answer: (SHOW ANSWER)

The first step for the user to take if virus infection is suspected is to report the incident to service desk. This will help to contain the infection, prevent further damage, and initiate the recovery process. The service desk can also provide guidance on how to handle the infected computer and what actions to take next. Unplugging the computer from the network, saving the opened files and shutting down the computer, or updating the antivirus to the latest version are possible subsequent steps, but they should not be done before reporting the incident.

NEW QUESTION: 160

電腦生成證據中最關鍵的方面是什麼？

A. 客觀性

B. 誠信

C. 及時性

D. 相關性

Answer: B (LEAVE A REPLY)

Integrity is the most critical aspect of computer-generated evidence. Integrity means that the evidence has not been altered, tampered, or corrupted in any way, and that it reflects the original state of the data or system. Integrity can be ensured by using cryptographic techniques, such as hashing, digital signatures, and encryption, as well as by following proper chain of custody and documentation procedures. Integrity is essential for the admissibility and reliability of the evidence in a court of law or an investigation.

NEW QUESTION: 161

以下哪□最能描述“特□蔓延”？

A. □特定已批准□目特意授予的一次性□先通行□

B. 用□随着□□的推移逐□□累不必要的□□□限，通常是由于用□角色□更或承担□□□□□，没有事先妥善撤□不再需要的□□□限。

C. 攻□者在主□攻□期□用于提升□限的一种技□

D. 申□新□□□限的正式流程

Answer: B (LEAVE A REPLY)

Privilege creep refers to the gradual, often unintentional accumulation of unnecessary access rights and permissions by a user over time-commonly occurring as an employee changes roles, departments, or takes on temporary project responsibilities without having their previous, no- longer-needed access properly reviewed and revoked-violating the principle of least privilege and increasing organizational risk, which periodic access reviews and recertification processes are designed to address.

NEW QUESTION: 162

某組織缺乏資料保留政策。下列哪位人士最適合就此需求提供諮詢？

A. 應用程式管理員

B. 資料庫管理員

C. 隱私官
D. 財務經理
Answer: C (LEAVE A REPLY)
The best person to consult for a data retention policy requirement is the privacy officer, who is responsible for ensuring that the organization complies with the applicable privacy laws, regulations, and standards. A data retention policy defines the criteria and procedures for retaining, storing, and disposing of data, especially personal data, in accordance with the legal and business requirements. The privacy officer can advise on the data retention policy by identifying the relevant privacy mandates, assessing the data types and categories, determining the retention periods and disposal methods, and implementing the appropriate controls and measures.

NEW QUESTION: 163
在設計網路資訊系統(IS)時，如果存在幾種不同類型的個人存取權限，那麼為了確保滿足所有存取控制要求，應該採取的第一步是什麼？
A. 建立使用者設定檔。
B. 建立使用者存取矩陣。
C. 制定存取控制清單(ACL)。
D. 制定基於角色的存取控制(RBAC)清單。
Answer: B (LEAVE A REPLY)
The first step to take when designing a networked Information System (IS) where there will be several different types of individual access is to create a user access matrix. A user access matrix is a table that defines the access rights and permissions of each user or user group to each resource or function in the system. A user access matrix helps to ensure that all access control requirements are addressed, such as the principle of least privilege, the principle of separation of duties, and the principle of need to know. A user access matrix also helps to simplify and standardize the implementation and administration of access control policies and mechanisms.

NEW QUESTION: 164
□看安全性日誌時，管理登入事件顯示的密碼是或”
"1'='1'--。這是以下哪種攻擊的範例？
A. 暴力攻擊
B. 結構化□詢語言 (SQL) 注入
C. 跨站□本 (XSS)
D. 彩虹表攻擊
Answer: B (LEAVE A REPLY)
The password ' OR ' '1'='1' -- is an example of a Structured Query Language (SQL) Injection attack. In this case, the string is designed to manipulate a SQL query by injecting SQL syntax into the login query. The ' OR '1'='1' -- part of the string forces the query to always evaluate to true ('1'='1'), allowing an attacker to bypass authentication mechanisms and log in without knowing the actual password. So the correct answer is B.

NEW QUESTION: 165
下列哪一項可以最大限度地減少攻擊者利用緩衝區溢位的能力？
A. 記憶體回顧
B. 程式碼審□
C. 訊息劃分
D. 緩衝區劃分
Answer: B (LEAVE A REPLY)
A code review involves thoroughly examining the software's source code to identify vulnerabilities, including potential buffer overflow issues. During a code review, developers can look for unsafe coding practices, such as improper bounds checking or unvalidated user inputs, that could lead to buffer overflows. By identifying these issues during the development phase, it is possible to fix them before the code is deployed, thereby minimizing the risk of exploitation.

NEW QUESTION: 166
一家公司正計劃實施私有雲基礎設施。下列哪些建議將支援遷移到雲端基礎架構？
A. 為每個部門實作虛擬區域網路 (VLAN)，並為每個VLAN 建立單獨的子網路。
B. 實施軟體定義網路 (SDN)，為網路基礎設施提供與控制和資料平面整合的能力。
C. 實作虛擬區域網路 (VLAN)，以邏輯上將區域網路(LAN) 與實體交換器分開。
D. 實施軟體定義網路 (SDN)，以提供應用進階策略來根據使用者 裝置和應用程式調整和重新排序網路流量的能力。
Answer: B (LEAVE A REPLY)
Implementing software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes is the recommendation that will support the move to a cloud infrastructure. A cloud infrastructure is a network architecture that provides on-demand access to shared and scalable resources and services over the Internet, such as computing, storage, networking, or applications. A cloud infrastructure can be classified into different service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), and into different deployment models, such as public cloud, private cloud, hybrid cloud, or community cloud. A private cloud is a type of cloud infrastructure that is owned, operated, and used by a single organization, and that is hosted on the organization's premises or on a third-party provider's premises. Implementing software- defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes is the recommendation that will support the move to a cloud infrastructure, because it can provide the following benefits:
It can decouple the network control plane from the data plane, and enable the network to be programmatically configured and managed by a centralized software controller, which can improve the flexibility, efficiency, and performance of the network.
It can dynamically adjust the network according to the policies and requirements of the cloud services and applications, and optimize the network resources and bandwidth allocation, which can enhance the scalability, reliability, and availability of the cloud infrastructure.

It can implement the security controls and measures at the network level, and monitor and protect the network traffic and communication, which can increase the security and privacy of the cloud infrastructure.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 167
醫院的樓宇控制系統監控和操作環境設備，以維持安全舒適的環境 下列哪一項可用於最大限度地降低公用事業供應中斷的風險？
A. 數位設備，可以關閉設備並持續快速循環，以增加供應並隱藏醫院網路上的活動
B. 標準化樓宇控制系統軟體，與醫院網路具有高連接性
C. 阻止維修人員存取可能影響關鍵公用設施供應的樓宇控制系統
D. 數位保護和控制設備，能口最大限度地減少對關鍵公用事業的不利影響
Answer: (SHOW ANSWER)
The best option to minimize the risk of utility supply interruption for a hospital's building controls system is to use digital protection and control devices capable of minimizing the adverse impact to critical utility. Digital protection and control devices are devices that monitor and regulate the utility supply, such as electricity, water, or gas, and detect and respond to any faults, anomalies, or disruptions in the utility supply. Digital protection and control devices can minimize the adverse impact to critical utility by isolating the affected components, switching to alternative sources, adjusting the load or demand, or activating backup or emergency systems. Digital protection and control devices can help to ensure the continuity and reliability of the utility supply, and to prevent or mitigate any potential damage or harm to the hospital's building controls system, or to the patients and staff.

NEW QUESTION: 168
在資料庫的高可用性(HA)選項中，哪個選項允許多個客口端同時存取多個資料庫伺服器？
A. 非結構化口詢語言(NoSQL)資料庫
B. 關聯式資料庫
C. 影子資料庫
D. 複製資料庫
Answer: D (LEAVE A REPLY)
A replicated database is a high availability (HA) option of database that allows multiple clients to access multiple database servers simultaneously. A replicated database is a database that is copied and distributed across multiple servers, usually in different locations. Replication ensures that the data is consistent and synchronized across all servers, and provides fault tolerance, load balancing, and

improved performance. Replication can be done in different modes, such as synchronous, asynchronous, or mixed.

NEW QUESTION: 169
下列哪一項措施可以保護傳輸層的 Web 交易安全性？
A. 安全超文本傳輸協定(S-HTTP)
B. 安全通訊端層 (SSL)
C. 套接字安全(SOCKS)
D. 安全外殼(SSH)
Answer: B (LEAVE A REPLY)
Secure Sockets Layer (SSL) is the only option that secures web transactions at the transport layer of the OSI model. SSL is a protocol or a standard that provides security and privacy for the data or the messages exchanged between a web browser and a web server, or between any two applications that use the TCP/IP protocol. SSL uses cryptographic techniques, such as encryption, decryption, hashing, and digital signatures, to protect the confidentiality, integrity, and authenticity of the data or the messages. SSL also uses certificates and public key infrastructure (PKI) to establish the identity and the trustworthiness of the parties involved in the web transactions.

NEW QUESTION: 170
下列哪一項是特權身分生命週期管理的必要要素？
A. 定期執行帳口重新驗證和審批
B. 基於多因素身份驗證的帳口配置
C. 經常審口已執行的活動並要求提供理由
D. 主管或直線主管需提供的帳口資訊
Answer: A (LEAVE A REPLY)
A privileged identity lifecycle management is a process of managing the access rights and activities of users who have elevated permissions to access sensitive data or resources in an organization. An essential element of a privileged identity lifecycle management is to regularly perform account re-validation and approval, which means verifying that the privileged users still need their access rights and have them approved by the appropriate authority. This can help prevent unauthorized or excessive access, reduce the risk of insider threats, and ensure compliance with policies and regulations. Account provisioning based on multi-factor authentication, frequently review performed activities and request justification, and account information to be provided by supervisor or line manager are also important aspects of a privileged identity lifecycle management, but they are not as essential as account re-validation and approval.

NEW QUESTION: 171
下列哪一項是防止攻擊者停用網路最有效的策略？
A. 測試業務連續性和災難復原 (DR) 計畫。
B. 設計具有適應、重新配置和故障轉移能力的網路。
C. 實施網路分段以實現穩健性。

D. 遵循安全準則以防止未經授權的網路存取。

Answer: (SHOW ANSWER)

The most effective strategy to prevent an attacker from disabling a network is to design networks with the ability to adapt, reconfigure, and fail over. A network that can adapt, reconfigure, and fail over is a network that can dynamically adjust its topology, configuration, and routing, and switch to alternative or backup components, in response to any changes, disruptions, or attacks in the network environment. A network that can adapt, reconfigure, and fail over can prevent an attacker from disabling a network, as it can maintain the availability, resilience, and performance of the network, and mitigate the impact or damage of the attack.

NEW QUESTION: 172

儲存區域網路 (SAN) 上的靜態資料位於開放系統互連 (OSI) 模型的哪個層級？

A. 連結層

B. 物理層

C. 會話層

D. 應用層

Answer: (SHOW ANSWER)

Data at rest on a Storage Area Network (SAN) is located at the physical layer of the Open System Interconnection (OSI) model. The OSI model is a conceptual framework that describes how data is transmitted and processed across different layers of a network. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The physical layer is the lowest layer of the OSI model, and it is responsible for the transmission and reception of raw bits over a physical medium, such as cables, wires, or optical fibers. The physical layer defines the physical characteristics of the medium, such as voltage, frequency, modulation, connectors, etc. The physical layer also deals with the physical topology of the network, such as bus, ring, star, mesh, etc.

A Storage Area Network (SAN) is a dedicated network that provides access to consolidated and block-level data storage. A SAN consists of storage devices, such as disks, tapes, or arrays, that are connected to servers or clients via a network infrastructure, such as switches, routers, or hubs. A SAN allows multiple servers or clients to share the same storage devices, and it provides high performance, availability, scalability, and security for data storage. Data at rest on a SAN is located at the physical layer of the OSI model, because it is stored as raw bits on the physical medium of the storage devices, and it is accessed by the servers or clients through the physical medium of the network infrastructure.

NEW QUESTION: 173

在嘗試避免敏感資料外洩時，應遵循下列哪一項最佳指南？

A. 僅在必要時儲存敏感資料。

B. 對最終使用者進行敏感資料攻擊方法的教育。

C. 為敏感資料建立報告參數。

D. 監視郵件伺服器是否有敏感資料外洩。

Answer: A (LEAVE A REPLY)

The best guideline to follow when attempting to avoid the exposure of sensitive data is to store sensitive data only when necessary. Sensitive data is a type of data or information that is considered or classified as confidential, private, or secret, and that can cause harm or damage to the data owner or the data subject, or to the organization or the business, if it is accessed or disclosed by unauthorized parties, such as hackers, insiders, or competitors. Sensitive data can include various types or categories, such as personal data, financial data, health data, or intellectual property data. Sensitive data can be exposed or revealed by various methods, such as a breach, which is a type of incident or event that occurs on a system or a network, and that results in the unauthorized access or disclosure of the sensitive data, and that compromises the confidentiality, integrity, or availability of the sensitive data. Sensitive data can be protected or secured by various methods, such as a guideline, which is a type of rule or principle that provides the direction, instruction, or recommendation for handling or managing the sensitive data, and that can be used as a reference or a standard for measuring or evaluating the compliance or alignment with the security requirements or regulations. Storing sensitive data only when necessary is a guideline that can be followed when attempting to avoid the exposure of sensitive data, as it can provide the benefits of both minimizing and securing the sensitive data, such as reducing the attack surface and exposure of the sensitive data, and enhancing the performance and security of the system or the network.

NEW QUESTION: 174
從安全性角度來看，下列哪一項是設定網域名稱服務(DNS) 系統的最佳實務？
A. 設定輔助伺服器以使用主伺服器作為區域轉發器。
B. 阻止所有傳輸控制協定 (TCP) 連線。
C. 停用名稱伺服器上的所有遞歸口詢。
D. 限制區域傳送到授權裝置。
Answer: (SHOW ANSWER)
From a security perspective, the best practice to configure a DNS system is to limit zone transfers to authorized devices. Zone transfers are the processes of replicating the DNS data from one server to another, usually from a primary server to a secondary server. Zone transfers can expose sensitive information about the network topology, hosts, and services to attackers, who can use this information to launch further attacks. Therefore, zone transfers should be restricted to only the devices that need them, and authenticated and encrypted to prevent unauthorized access or modification.

NEW QUESTION: 175
進行安全評估最重要的目標是什麼？
A. 為組織進行外部審計（尤其是監管機構的外部審計）做好準備
B. 發現未緩解的安全漏洞，並提出緩解這些漏洞的路徑
C. 使安全計畫與組織風險偏好一致
D. 向高階管理層展示安全控制和流程的正確功能
Answer: (SHOW ANSWER)
The most important goal of conducting security assessments is to discover unmitigated security vulnerabilities, and propose paths for mitigating them. A security assessment is a process that involves

evaluating and testing the security posture and performance of a system or network, and identifying and reporting any security vulnerabilities or issues that may pose a security risk. A security assessment can help to discover unmitigated security vulnerabilities, which are the security flaws or weaknesses that have not been detected, reported, or resolved, and that can be exploited by the adversaries to compromise the security of the system or network. A security assessment can also help to propose paths for mitigating the security vulnerabilities, which are the actions or measures that can be taken to eliminate, reduce, or transfer the security risk associated with the security vulnerabilities. Discovering unmitigated security vulnerabilities, and proposing paths for mitigating them, is the most important goal of conducting security assessments, as it can help to improve the security level and quality of the system or network, and to prevent or minimize the potential damage or loss caused by the security incidents or breaches.

NEW QUESTION: 176
作為軟體開發生命週期 (SDLC) 的一部分，誰應該執行設計審口以發現安全設計缺陷？
A. 企業主
B. 安全主題專家 (SME)
C. 應用程式擁有者
D. 開發者主題專家 (SME)
Answer: (SHOW ANSWER)
A security subject matter expert (SME) should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC). A security SME has the knowledge and experience to identify and mitigate potential security risks and vulnerabilities in the design phase, before they become costly and difficult to fix in later stages. The business owner, the application owner, and the developer SME may not have the sufficient security expertise or perspective to conduct a thorough and effective design review.

NEW QUESTION: 177
使用者帳口配置必須提供下列哪些資訊？
A. 全名
B. 唯一識別符
C. 安全性問題
D. 出生日期
Answer: B (LEAVE A REPLY)
For user account provisioning, the essential information that must be provided is typically aimed at ensuring proper identification and uniqueness of each user account in the system.

NEW QUESTION: 178
程式碼簽名的目的是什麼？
A. 簽署者驗證正在載入的軟體是否為簽署者原創的軟體。
B. 供應商證明正在載入的軟體沒有惡意程式碼，並且是由簽署者發起的
C. 簽署者驗證正在載入的軟體是否不含惡意程式碼。

D. 供應商和簽署者都證明正在載入的軟體沒有惡意程式碼，並且由簽署者發起。

Answer: B (LEAVE A REPLY)

The statement that best describes the purpose of a digital signature is that the vendor certifies the software being loaded is free of malicious code and that it was originated by the signer. A digital signature is a type of electronic signature that uses a cryptographic technique to verify the authenticity, integrity, and non-repudiation of a digital document, such as a software, message, or transaction. A digital signature is created by applying a hash function and a private key to the digital document, and it is verified by using a public key and a certificate. A digital signature can help to certify that the software being loaded is free of malicious code and that it was originated by the signer, by ensuring that the software has not been altered or tampered with since it was signed, and that the signer is the legitimate and authorized source of the software. The signer verifies that the software being loaded is the software originated by the signer, the signer verifies that the software being loaded is free of malicious code, or both vendor and the signer certify the software being loaded is free of malicious code and it was originated by the signer are not the statements that best describe the purpose of a digital signature, as they are either inaccurate, incomplete, or redundant statements about the digital signature.

NEW QUESTION: 179

一位網路安全工程師的任務是研究並實施一個超安全的通訊管道，以保護組織最有價口的智慧財口權(IP)。該計劃的首要目標是確保通訊口對不會被攔截而不被發現。下列哪一項是確保實現此目標的唯一方法？

A. Diffie-Hellman金鑰交換

B. 對稱金鑰密碼學

C. [公鑰基礎設施(PKI)

D. 量子金鑰分發

Answer: D (LEAVE A REPLY)

The only way to ensure an ultra-secure communications channel that cannot be intercepted without detection is to use Quantum Key Distribution (QKD). QKD is a technique that uses the principles of quantum mechanics to generate and exchange cryptographic keys between two parties. QKD relies on the properties of quantum particles, such as photons or electrons, to encode and transmit the keys. QKD offers the following advantages for securing communications:

It provides unconditional security, as the keys are generated and exchanged in a random and unpredictable manner, and cannot be computed or guessed by any algorithm or attacker.

It ensures perfect secrecy, as the keys are used only once and then discarded, and cannot be reused or intercepted by any eavesdropper.

It enables detection of intrusion, as any attempt to observe or measure the quantum particles will alter their state and introduce errors or anomalies in the communication, which can be noticed and reported by the legitimate parties. QKD is currently limited by the distance, speed, and cost of the quantum communication channels, but it is expected to become more feasible and widespread in the future, especially with the development of quantum networks and quantum computers.

NEW QUESTION: 180
下列哪一項描述了最佳配置管理實務？
A. 安裝新系統後，設定檔將複製到單獨的備份系統並進行雜湊處理以偵測□改。
B. 安裝新系統後，設定檔將複製到氣隙系統並進行雜湊處理以偵測□改。
C. 防火牆規則備援到氣隙系統。
D. 為所有相關係統建立和維護基線配置。
Answer: D (LEAVE A REPLY)
The best configuration management practice is to create and maintain a baseline configuration for all relevant systems. A baseline configuration is a documented and approved set of specifications and settings for a system or component that serves as a standard for comparison and evaluation. A baseline configuration can help ensure the consistency, security, and performance of the system or component, as well as facilitate the identification and resolution of any deviations or issues. A baseline configuration should be updated and reviewed regularly to reflect the changes and improvements made to the system or component

NEW QUESTION: 181
以下哪□最能描述"供□商□定"作□云□算□□的作用？
A. 供□商无法□展服□□模以□足需求
B. 由于□有技□、格式或高昂的□□成本，□以将数据 □用程序或工作□□从云提供商迁移出去。
C. 供□商未能提供足□的客□支持
D. 一□要求□行年度安全□□的合同条款
Answer: B (LEAVE A REPLY)
Vendor lock-in occurs when an organization becomes highly dependent on a specific cloud provider's proprietary technologies, APIs, or data formats, making it difficult, costly, or time- consuming to migrate to a different provider or bring workloads back in-house, which should be considered during vendor selection and architecture design.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 182
負責處理機密資料的系統的應用程式負責人離職。預計大約六個月後會招募到替代人選。在此期間，組織應該採取下列哪一項措施？
A. Gram 暫時存取原始應用程式擁有者的帳□
B. 為系統指派一個臨時應用程式擁有者。

C. 限制對系統的訪問，直到聘請到新的應用程式擁有者。
D. 在聘請新的應用程式擁有者之前，防止對機密資料進行更改。
Answer: B (LEAVE A REPLY)
When the application owner of a system that handles confidential data leaves an organization, it is essential to maintain proper oversight and management of the system to ensure security, compliance, and continuity of operations. The best approach during the interim period is to assign a temporary application owner who can manage the system's day-to-day operations and ensure it remains secure, compliant, and functional until the new permanent application owner is hired.
This temporary application owner will be responsible for:
Overseeing the system's security.
Ensuring access controls and data protection measures are maintained.
Monitoring the system for any issues or vulnerabilities.
Keeping track of any necessary updates or patches.

NEW QUESTION: 183
以下哪□最能描述□□拉帕杜拉模型的“星形属性”(-属性)？
A. 受控□象无法□取比自身□限□□更高的数据。
B. 用□无法将数据写入低于自身□限□□的密□，从而防止数据向下流至□限□低的□□。
C. 任何分□□□的主体都可以自由□□和写作。
D. □象的□限□□与其写入□限无关。
Answer: B (LEAVE A REPLY)
The Star Property (-property), also known as the "no write down" rule, prevents a subject from writing data to an object at a lower classification level than their own current clearance, preventing sensitive information from being inadvertently or maliciously disclosed to a less trusted level, complementing the Simple Security Property's "no read up" rule.

NEW QUESTION: 184
下列哪些服務可以透過雲端服務或本地部署來與身分即服務 (IDaaS) 整合作為使用者身分的權威來源？
A. 目錄
B. 使用者資料庫
C. 多重驗證 (MFA)
D. 單一登入 (SSO)
Answer: (SHOW ANSWER)
A directory service can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities. A directory service is a software application that stores and organizes information about the users, devices, and resources in a network. A directory service provides a centralized and standardized way to manage and access the information, and to perform identity and access management functions, such as authentication, authorization, and auditing. A directory service uses a hierarchical or tree- like structure to organize the information into logical units, such as domains, organizational units, or groups. A directory service also uses a schema

to define the attributes and rules for the information, such as the name, password, or role of a user. A directory service can be deployed via a cloud service or on-premises, depending on the needs and preferences of the organization.
A cloud-based directory service is a directory service that is hosted and managed by a cloud service provider, such as Azure Active Directory or Google Cloud Directory. A cloud-based directory service can offer the advantages of scalability, availability, and cost-effectiveness, but may also pose the challenges of security, privacy, and compliance. An on-premises directory service is a directory service that is installed and managed by the organization itself, such as Microsoft Active Directory or OpenLDAP. An on-premises directory service can offer the advantages of control, customization, and integration, but may also pose the challenges of maintenance, performance, and reliability. A directory service can be integrated with IDaaS as the authoritative source of user identities. IDaaS is a cloud-based service that provides identity and access management capabilities, such as single sign-on, multi-factor authentication, or identity federation, to the users and applications of an organization. IDaaS can leverage the existing user information and credentials from the directory service, and synchronize and authenticate them across different systems and platforms. IDaaS can also provide additional features and functions that the directory service may not support, such as self-service, password management, or identity governance.

NEW QUESTION: 185
以下哪□最能描述“出口点数据最小化”作□□私原□的目的？
A. 收集并保留尽可能多的数据，以□将来潜在使用。
B. □收集、□理和保留□□□特定、明确目的所必需的最低限度的个人或敏感数据，从而降低整体□私□□和泄露□□。
C. 无□数据是否必要，都□其□行加密
D. 一种□□用于□化数据□□□性能的技□
Answer: B (LEAVE A REPLY)
Data minimization is a core privacy principle (reflected in regulations such as GDPR) requiring organizations to collect, process, and retain only the minimum amount of personal or sensitive data actually necessary to achieve a specific, clearly defined purpose, reducing the overall volume of data at risk in the event of a breach and limiting unnecessary privacy exposure.

NEW QUESTION: 186
使用網路瀏覽器存取雲端的服務時，主要關注下列哪一項？
A. 應用程式介面 (API) 的不安全實現
B. 管理金鑰使用與儲存不當
C. 基礎設施配置錯誤，導致未經授權的訪問
D. 協定中可能洩漏機密資料的漏洞
Answer: (SHOW ANSWER)
The primary concern when using an Internet browser to access a cloud-based service is the vulnerabilities within protocols that can expose confidential data. Protocols are the rules and formats that govern the communication and exchange of data between systems or applications.

Protocols can have vulnerabilities or flaws that can be exploited by attackers to intercept, modify, or steal the data. For example, some protocols may not provide adequate encryption, authentication, or integrity for the data, or they may have weak or outdated algorithms, keys, or certificates. When using an Internet browser to access a cloud-based service, the data may be transmitted over various protocols, such as HTTP, HTTPS, SSL, TLS, etc. If any of these protocols are vulnerable, the data may be compromised, especially if the data is sensitive or confidential. Therefore, it is important to use secure and updated protocols, as well as to monitor and patch any vulnerabilities

NEW QUESTION: 187
如果實施口容管理系統 (CMC)，會發生下列哪一項？
A. 開發人員將無法再存取生口系統
B. 投入生口的應用程式是安全的
C. 修補系統會更快完成
D. 測試和生口系統將運行相同的軟體
Answer: (SHOW ANSWER)
If a content management system (CMS) is implemented, one of the outcomes would be that the test and production systems would be running the same software. A CMS is a software application that is used to create, manage, and deliver digital content, such as web pages, blogs, or documents. A CMS typically consists of two components: the content management application (CMA) and the content delivery application (CDA). The CMA is the front-end interface that allows users to create, edit, and organize the content. The CDA is the back-end component that stores, processes, and delivers the content to the end-users. A CMS can simplify and streamline the content creation and delivery process, by providing a consistent and standardized platform for both the test and production systems. A CMS can also ensure the quality, security, and availability of the content, by providing features such as version control, access control, backup, and recovery.

NEW QUESTION: 188
使用具有身分驗證標頭 (AH) 的虛擬私人網路 (VPN) 時，可提供下列哪一項保護？
A. 負載加密
B. 寄件者機密性
C. 寄件者不可否認性
D. 多重驗證 (MFA)
Answer: C (LEAVE A REPLY)
A VPN is a secure tunnel that connects two or more networks over a public network, such as the internet. VPNs use encryption and authentication protocols to protect the data in transit from unauthorized access, modification, or disclosure. AH is one of the protocols used by IPsec, which is a suite of protocols for securing IP traffic. AH provides integrity, authentication, and anti-replay protection for the entire IP packet, including the header and the payload. AH does not provide payload encryption or sender confidentiality, which are provided by another IPsec protocol called Encapsulating Security Payload (ESP). AH also does not provide multi-factor authentication (MFA), which is a method of verifying the identity of a user or a device by requiring two or more factors, such as something you

know, something you have, or something you are. AH does provide sender non-repudiation, which is the assurance that the sender of a message cannot deny sending it, because the message is authenticated with a digital signature or a keyed hash that only the sender can generate.

NEW QUESTION: 189
服裝零售商員工擁有用□帳□，可以存取合作夥伴企業的資源。所有合作夥伴企業都使用通用身分和存取管理 (IAM) 協定和不同的技術。根據擴展身分原則，合作夥伴企業之間允許此TAM 操作的流程是什麼？
A. 服裝零售商充當身分提供者 (IdP)，使用行業標準確認使用者身份，然後將憑證發送給充當服務提供者並允許存取服務的合作夥伴企業。
B. 服裝零售商充當使用者自助服務，使用業界標準確認使用者身份，然後將憑證發送給充當服務提供者並允許存取服務的合作夥伴企業。
C. 服裝零售商充當服務提供者，使用業界標準確認使用者身份，然後將憑證傳送給充當身分提供者(IdP)並允許存取資源的合作夥伴企業。
D. 服裝零售商充當存取控制提供者，使用業界標準確認使用者的存取權限，然後將憑證發送給充當服務提供者並允許存取資源的合作夥伴企業。
Answer: A (LEAVE A REPLY)
The Extended Identity principle is a concept that describes how an organization can extend its identity and access management (IAM) capabilities to external entities, such as customers, partners, or suppliers, by using common standards and protocols, such as SAML, OAuth, or OpenID Connect. Under this principle, the clothing retailer acts as an identity provider (IdP), which is the entity that authenticates and verifies the identity of the user using industry standards, such as passwords, tokens, or biometrics. The partner businesses act as service providers (SPs), which are the entities that provide access to the resources or services that the user requests, such as inventory, shipping, or payment. The clothing retailer sends the credentials of the user, such as a SAML assertion or an OAuth token, to the partner businesses, which use them to grant access to the user. This way, the user does not need to create or manage multiple accounts or passwords for each partner business, and the clothing retailer can maintain control and visibility over the user's identity and access.

NEW QUESTION: 190
以下哪□最能描述“出口点加密流量分析 (ETA)”在不□行完全解密的情况下的目的？
A. 完全解密所有流量，以明文形式□□其内容
B. 分析加密流量的元数据和□□模式(例如数据包大小、□□和流特征)，以□□潜在的□意活□，而无需解密□□有效□荷。
C. 默□阻止所有加密流量
D. □了便于□□，用□弱的密□替□了原有的加密算法。
Answer: B (LEAVE A REPLY)
Encrypted Traffic Analysis uses machine learning and statistical analysis of observable metadata- such as packet size distributions, timing patterns, and flow characteristics-to identify potentially malicious traffic (such as malware command-and-control communication) within encrypted connections, without

requiring full decryption of the payload, preserving privacy while still enabling some level of threat detection.

NEW QUESTION: 191
確定組織中的任務關鍵資口最有效的方法是什麼？
A. 漏洞分析
B. 業務流程分析
C. 威脅分析
D. 業務風險分析
Answer: B (LEAVE A REPLY)
Business process analysis is the most effective way to determine a mission critical asset in an organization. Business process analysis is a method of identifying, documenting, and optimizing the core business processes that deliver value to the customers and stakeholders. By analyzing the business processes, an organization can identify the assets that are essential for the successful operation and continuity of the business, such as data, systems, personnel, facilities, and suppliers. These assets are then classified as mission critical and prioritized for protection and recovery.

NEW QUESTION: 192
下列哪一項最能描述殭屍網路？
A. 網路上的電腦系統，旨在誘捕試圖滲透其他電腦系統的人
B. 一組相關程序，用於保護專用網路的資源免受其他網路的影響
C. 插入組織專用網路和外部公共網路之間的中立區域的小型網絡
D. 用於發動破壞性攻擊的電腦組
Answer: D (LEAVE A REPLY)
A botnet is a network of compromised computers (often referred to as "bots" or "zombies") that are controlled remotely by an attacker (often called a botmaster). These computers are typically infected with malware that allows the attacker to control them without the owner's knowledge.
Once a botnet is created, it can be used to launch a variety of destructive attacks, such as:
Distributed Denial of Service (DDoS) attacks, where the botnet overwhelms a target server with traffic.
Spamming, where the botnet is used to send out vast numbers of unwanted emails.
Data theft, where the botnet is used to steal sensitive information from compromised computers.
Malware distribution, where the botnet is used to propagate malware to other systems.
Botnets are used for malicious purposes and are a significant security threat on the internet.

NEW QUESTION: 193
下列哪一項封裝了全碟加密實作的解密金鑰，並將硬碟綁定到特定裝置？
A. 可信任平台模組(TPM)
B. 預口動執行環境 (PXE)
C. 金鑰分發中心(KDC)
D. 網際網路協定簡易金鑰管理(SKIP)
Answer: A (LEAVE A REPLY)

A Trusted Platform Module (TPM) is a hardware-based security feature that can be used to securely store cryptographic keys, such as the decryption key for full disk encryption (FDE). It provides a secure environment that is resistant to tampering and can bind the decryption key to the specific hardware of the device. This way, the decryption key is not stored in a way that can be easily extracted by an attacker, and the disk is tied to the particular device, ensuring that the data remains inaccessible if the device is moved to another machine.

NEW QUESTION: 194
以下哪□最能描述“分布式拒□服□ (DDoS) 攻□”？
A. 由□一来源□起的、□□□一漏洞的攻□
B. 一种利用多个被入侵系□(通常构成僵尸网□)向目□系□□起攻□，通□大量流量淹没目□并破坏其可用性的攻□。
C. 利用 SQL 注入漏洞的攻□
D. 一种完全依□社会工程学的攻□
Answer: B (LEAVE A REPLY)
A DDoS attack leverages numerous compromised systems (often forming a botnet) distributed across different locations to simultaneously flood a target with traffic or requests, overwhelming its resources and causing a denial of service that is typically much harder to mitigate than an attack from a single source.

NEW QUESTION: 195
下列哪一種攻擊如果成功，可以讓入侵者完全控制軟體定義網路(SDN) 架構？
A. 嗅探網路□受感染主機的流量
B. 傳送控制訊息以開□來自網路□受感染主機的不通過防火牆的串流
C. 對控制器的 Secure Shell (SSH) 連接埠進行暴力密碼攻擊
D. 遠端驗證撥入使用者服務 (RADIUS) 令牌重播攻擊
Answer: (SHOW ANSWER)
A brute force password attack on the SSH port of the controller is the attack that, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture. SDN is a networking architecture that decouples the control plane from the data plane, and centralizes the network intelligence and management in a software-based controller. The controller is the core component of the SDN architecture, and it communicates with the network devices and applications through standardized protocols, such as OpenFlow. The controller is responsible for configuring, monitoring, and optimizing the network performance and behavior, and it provides a global view and control of the network. A brute force password attack is a type of attack that involves trying different combinations of passwords or keys until the correct one is found. A brute force password attack on the SSH port of the controller could allow an intruder to gain unauthorized access to the controller, and to compromise the security and functionality of the entire SDN architecture. The intruder could manipulate the network configuration and policies, disrupt the network traffic and services, steal or modify the network data, or launch further attacks on the network devices and applications.

NEW QUESTION: 196
最近在組織的網路上實施了使用質詢和回應的身份驗證系統，因為該組織進行了年度滲透測試，表明測試人員能□使用經過身份驗證的憑證進行橫向移動。最有可能使用哪種攻擊方法來實現此目的？
A. 跨站□本 (XSS)
B. 傳票
C. 暴力破解
D. 哈希衝突
Answer: B (LEAVE A REPLY)
Pass the ticket is an attack method that exploits the Kerberos authentication protocol, which is a network authentication protocol that uses tickets to authenticate users and services. In a pass the ticket attack, an attacker steals a valid Kerberos ticket from a compromised user or system, and uses it to impersonate the user or system and access other resources or services on the network, without knowing the user's password or credentials. This attack can enable the attacker to move laterally across the network and escalate privileges. An authentication system that uses challenge and response, which is a method of verifying the identity of a user or system by sending a random or unpredictable value (challenge) and expecting a valid response (such as a password or a hash), can prevent or mitigate the pass the ticket attack, as it requires the user or system to prove their knowledge of the secret value, not just possession of the ticket.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 197
利用社會工程和惡意統一資源定位器 (URL) 連結來利用受害者與 Web 應用程式的現有瀏覽器會話的攻擊是以下哪種攻擊類型的範例？
A. 跨站□本 (XSS)
B. 跨站請求偽造 (CSRF)
C. 注入
D. 點擊劫持
Answer: B (LEAVE A REPLY)
An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of a cross-site request forgery (CSRF) attack. A CSRF attack is a type of web-based attack that exploits the trust between a web browser and a web server, by tricking the victim into performing an unwanted action on a web application that the victim is already authenticated or authorized to use. For example, a CSRF attack can make the victim transfer funds, change passwords, or delete accounts on a web application,

without the victim's knowledge or consent. A CSRF attack typically involves the following steps: The attacker crafts a malicious URL or HTML code that contains a forged request to a web application that the victim is likely to use, such as a banking, shopping, or social media site. The attacker delivers the malicious URL or HTML code to the victim, using social engineering techniques, such as phishing emails, instant messages, or web pages. The victim clicks on the malicious URL or HTML code, which is executed by the victim's web browser. The victim's web browser sends the forged request to the web application, along with the victim's session cookie or token, which authenticates or authorizes the victim to the web application. The web application receives the forged request and executes it, as if it was initiated by the victim. The web application performs the unwanted action, such as transferring funds, changing passwords, or deleting accounts, on behalf of the victim. Cross-Site Scripting (XSS), Injection, and Click jacking are not types of attacks that utilize social engineering and a malicious URL link to take advantage of a victim's existing browser session with a web application. XSS is a type of web-based attack that exploits the vulnerability of a web application, by injecting malicious scripts into the web pages that are viewed by other users. Injection is a type of web-based attack that exploits the vulnerability of a web application, by injecting malicious commands or queries into the user input, such as forms, fields, or URLs. Click jacking is a type of web-based attack that exploits the vulnerability of a web browser, by overlaying a transparent or hidden layer on top of a legitimate web page, and tricking the user into clicking on the hidden layer, which performs an unwanted action on the underlying web page.

NEW QUESTION: 198
下列哪一項是安全斷言標記語言(SAML)的功能？
A. 文件分配
B. 冗餘檢口
C. 擴充驗證
D. 政策執行
Answer: D (LEAVE A REPLY)
A function of Security Assertion Markup Language (SAML) is policy enforcement. SAML is an XML-based standard for exchanging authentication and authorization information between different entities, such as service providers and identity providers. SAML enables policy enforcement by allowing the service provider to specify the security requirements and conditions for accessing its resources, and allowing the identity provider to assert the identity and attributes of the user who requests access.

NEW QUESTION: 199
軟體掃描器在二口影像中辨識出一個高口區域。這最可能顯示什麼？
A. 加密例程
B. 隨機數口生器
C. 混淆程式碼
D. 殭屍網路指令與控制
Answer: C (LEAVE A REPLY)

Obfuscated code is a type of code that is deliberately written or modified to make it difficult to understand or reverse engineer. Obfuscation techniques can include changing variable names, removing comments, adding irrelevant code, or encrypting parts of the code. Obfuscated code can have high entropy, which means that it has a high degree of randomness or unpredictability.
A software scanner can identify a region within a binary image having high entropy as a possible indication of obfuscated code. Encryption routines, random number generators, and botnet command and control are not necessarily related to obfuscated code, and may not have high entropy.

NEW QUESTION: 200
下列哪一項是減少存取控制規避的最佳方法？
A. 獨立工作的多層存取控制
B. 多供應商技術實施方法
C. 口用網際網路通訊協定 (IP) 過濾的多層防火牆架構
D. 技術多樣化的多層存取控制
Answer: D (LEAVE A REPLY)
To mitigate circumvention of access controls, the best approach is to implement multi-layer access controls that use diversified technologies. This means combining different types of access control mechanisms (e.g., authentication, authorization, encryption, and physical security) that work together to strengthen the overall security posture. The diversification of technologies reduces the risk of an attacker bypassing all of them, as different technologies and strategies typically address different types of vulnerabilities.

NEW QUESTION: 201
關於等價類測試，下列哪一項敘述是正確的？
A. 測試輸入是從給定功能規範的派生邊界獲得的。
B. 其特徵是函數中實現的程序的無狀態行為。
C. 僅考慮該分割區中的一個代表口即可覆寫整個分割區。
D. 對於測試通訊協定和圖形使用者介面很有用。
Answer: C (LEAVE A REPLY)
An entire partition can be covered by considering only one representative value from that partition is a true statement regarding equivalence class testing. Equivalence class testing is a technique of software testing that divides the input domain of a function into partitions or classes that have the same expected output or behavior. By selecting only one representative value from each partition, the tester can reduce the number of test cases and still achieve high coverage and efficiency. Equivalence class testing is based on the assumption that if one value in a partition works correctly, then all other values in that partition will work correctly as well.

NEW QUESTION: 202
口什么网口管理口在口行网口分段口会口口分布式虚口交口机而不是独立交口机？
A. 采用口一供口商口准

B. □了最大限度地提高数据平面效率
C. 确保管理流量隔离
D. 降低配置□□的□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 203
以下哪□最能描述"数据脱敏"的目的？
A. 使用□个主密□加密整个数据□
B. □数据集中的特定数据元素□行模糊□理(例如，□□示信用卡号的后四位)，以保□敏感信息，同□保持其在非生□□境中的可用性。
C. 从数据□中永久□除敏感数据
D. □□数据□以减少存□需求
Answer: B (LEAVE A REPLY)
Data masking obscures or substitutes specific sensitive data elements within a dataset-such as showing only partial values or replacing them with realistic but fictitious data-while preserving the overall structure and usability of the data, commonly used to protect sensitive information in non-production environments like testing or development.

NEW QUESTION: 204
在傳輸控制協定/網際網路協定 (TCP/IP) 堆疊中，哪一層負責與另一個節點協商並建立連線？
A. 傳輸層
B. 應用層
C. 網路層
D. 會話層
Answer: A (LEAVE A REPLY)
The transport layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack is responsible for negotiating and establishing a connection with another node. The TCP/IP stack is a simplified version of the OSI model, and it consists of four layers: application, transport, internet, and link. The transport layer is the third layer of the TCP/IP stack, and it is responsible for providing reliable and efficient end-to-end data transfer between two nodes on a network. The transport layer uses protocols, such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), to segment, sequence, acknowledge, and reassemble the data packets, and to handle error detection and correction, flow control, and congestion control. The transport layer also provides connection-oriented or connectionless services, depending on the protocol used.
TCP is a connection-oriented protocol, which means that it establishes a logical connection between two nodes before exchanging data, and it maintains the connection until the data transfer is complete. TCP uses a three-way handshake to negotiate and establish a connection with another node. The three-way handshake works as follows:
The client sends a SYN (synchronize) packet to the server, indicating its initial sequence number and requesting a connection.

The server responds with a SYN-ACK (synchronize-acknowledge) packet, indicating its initial sequence number and acknowledging the client's request.
The client responds with an ACK (acknowledge) packet, acknowledging the server's response and completing the connection.
UDP is a connectionless protocol, which means that it does not establish or maintain a connection between two nodes, but rather sends data packets independently and without any guarantee of delivery, order, or integrity. UDP does not use a handshake or any other mechanism to negotiate and establish a connection with another node, but rather relies on the application layer to handle any connection-related issues.

NEW QUESTION: 205
以下哪□最能描述 API 网关上“出口点速率限制”的目的？
A. 自□加密 API 响□
B. 限制客□端在□定□□段内可以□出的□求数量，有助于减少□用 拒□服□攻□和□源耗尽的情况。
C. 使用 OAuth 令牌□ API 客□端□行身份□□
D. □□□入 API □求的模式
Answer: B (LEAVE A REPLY)
Rate limiting on an API gateway restricts the number of requests a client (identified by API key, IP address, or user account) can make within a specified time window, helping to protect backend resources from abuse, brute-force attempts, and denial-of-service conditions caused by excessive or malicious request volumes.

NEW QUESTION: 206
在從大型安全設施快速非緊急疏散期間，下列哪一項是最有效的機制來解釋所有員工的情況？
A. 大型陷阱，使用臉部辨識技術辨識離開的人群
B. 卡片□動旋轉門，人員在退出時進行驗證
C. 帶有推桿的緊急出口，每個出口處都有座標，根據預先定義的清單檢□個人
D. 每位員工所配戴的無線射頻辨識 (RFID) 感測器，由每個出口處的感測器掃描
Answer: (SHOW ANSWER)

NEW QUESTION: 207
為什麼網路管理員會選擇分散式虛擬交換器而不是獨立交換器來進行網路分段？
A. 針對單一供應商進行標準化
B. 確保管理流量的隔離
C. 最大化資料平面效率
D. 降低設定錯誤的風險
Answer: (SHOW ANSWER)
Reducing the risk of configuration errors is the reason why a network administrator might choose distributed virtual switches instead of stand-alone switches for network segmentation. Network segmentation is a technique that involves dividing a network into smaller and isolated segments or subnets, based on the criteria such as the function, the location, the security, or the performance.

Network segmentation can provide several benefits, such as improving the security, the efficiency, and the scalability of the network. Switches are the devices that are used to connect and communicate between the devices within a network segment or subnet, and to forward the data packets or frames to the appropriate destination. Switches can be either physical or virtual, and either stand-alone or distributed. A stand-alone switch is a switch that operates independently and separately from other switches, and that has its own configuration and management. A distributed switch is a switch that operates as a part of a group or a cluster of switches, and that shares the same configuration and management. A virtual switch is a switch that is implemented in software, and that runs on a virtual machine or a hypervisor. A distributed virtual switch is a virtual switch that operates as a part of a group or a cluster of virtual switches, and that shares the same configuration and management. A network administrator might choose distributed virtual switches instead of stand- alone switches for network segmentation, as distributed virtual switches can reduce the risk of configuration errors, which are the mistakes or the inconsistencies that may occur when setting up or modifying the parameters or the settings of the switches. Configuration errors can cause various problems or issues, such as the loss of connectivity, the degradation of performance, the exposure of vulnerabilities, or the violation of policies. Distributed virtual switches can reduce the risk of configuration errors, as they can provide a centralized and consistent way of configuring and managing the switches.

NEW QUESTION: 208
下列哪一項是隱私的共同特徵？
A. 維護私人資料存取審核追蹤的規定
B. 通知主題存在包含相關信用卡資料的資料庫
C. 主體現場檢口並修正個人資料的流程
D. 隱私資料整合的資料庫要求
Answer: B (LEAVE A REPLY)
A common characteristic of privacy is ensuring that individuals are informed about the collection and processing of their personal data. This is aligned with principles found in various privacy laws and frameworks, such as the General Data Protection Regulation (GDPR), which mandates that individuals (data subjects) be notified about how their personal data is collected, stored, and used. This process is often called data subject notification and ensures transparency and informed consent.
In the context of privacy, notice to individuals about the collection of their personal data (such as credit card information) is a key aspect of respecting their privacy rights.

NEW QUESTION: 209
使用感應卡進入建築物屬於哪種類型的安全控制？
A. 法律
B. 邏輯
C. 物理
D. 程序
Answer: C (LEAVE A REPLY)

The type of security control that is exemplified by the use of a proximity card to gain access to a building is physical. Physical security controls are the controls that protect the physical assets or resources of an organization, such as buildings, equipment, or documents, from unauthorized or malicious access, damage, or theft. Physical security controls can include locks, doors, windows, fences, gates, cameras, alarms, guards, or badges. A proximity card is a type of physical security control that uses a radio frequency identification (RFID) chip or a magnetic stripe to store and transmit the identity or the credentials of the card holder, and that can be used to unlock or open a door or a gate by bringing the card close to a reader or a scanner. Legal, logical, and procedural are not the types of security control that are exemplified by the use of a proximity card to gain access to a building, as they are related to the laws, regulations, or contracts, the software, hardware, or network components, or the policies, guidelines, or processes that govern the security of the organization's information systems or data, not the physical assets or resources.

NEW QUESTION: 210
採用企業範圍的業務連續性 (BC) 計畫需要下列哪一項？
A. 整個組織□良好的溝通
B. 完整的商業影響分析 (BIA)
C. 組成災難復原 (DR) 專案團隊
D. 有據可□的資訊資□分類
Answer: (SHOW ANSWER)
The adoption of an enterprise-wide Business Continuity (BC) program requires good communication throughout the organization, as it involves the coordination and collaboration of various stakeholders, such as senior management, business units, IT departments, and external partners. Good communication ensures that the BC program objectives, scope, roles, and responsibilities are clearly defined and understood by all parties, and that the BC program activities, such as Business Impact Analysis (BIA), risk assessment, strategy selection, plan development, testing, and maintenance, are effectively executed and monitored. Good communication also helps to raise the awareness and commitment of the organization to the BC program, and to foster a culture of resilience and preparedness.

NEW QUESTION: 211
安全團隊收到通知，網路上的裝置感染了惡意軟體 下列哪一項對於快速定位和修復設備最有效？
A. 資料遺失保護 (DLP)
B. 入侵偵測
C. 漏洞掃描器
D. 資訊科技資□管理 (ITAM)
Answer: D (LEAVE A REPLY)
Information Technology Asset Management (ITAM) is the most effective tool in enabling the device on the network to be quickly located and remediated. ITAM is a process that tracks and manages the inventory, configuration, and lifecycle of the IT assets in an organization, such as hardware, software, and network devices. ITAM can help to identify and locate the device that is infected with malware, by

providing information such as the device name, IP address, MAC address, serial number, location, owner, and status. ITAM can also help to remediate the device, by providing the necessary tools and procedures to isolate, quarantine, scan, clean, or replace the device.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 212
以下哪□最能描述与外部合作伙伴□行“出□点机密数据令牌化共享”的目的？
A. 直接与所有外部合作伙伴共享原始、未加密的敏感数据
B. 共享指向敏感数据的非敏感令牌，而非□□的原始敏感数据本身，从而允□外部合作伙伴在不直接□理或存□原始敏感信息的情况下□行必要的功能。
C. 一种□□共享□□内部的静□数据□行加密的方法
D. 一种□用于内部数据共享的技□，□不会与外部各方共享。
Answer: (SHOW ANSWER)
Tokenized sharing with external partners involves providing a non-sensitive token that references the original sensitive data (stored securely within the originating organization's token vault), rather than sharing the actual raw sensitive data directly, allowing external partners to perform necessary business functions (such as processing a transaction) without ever directly handling, storing, or being exposed to the original sensitive information, reducing overall data exposure and third-party risk.

NEW QUESTION: 213
以下哪□最能描述使用区□□或分布式□本技□□行“出□点数据溯源跟踪”的目的？
A. □使用□称算法□数据□行加密
B. □建不可□改、可□□的数据来源、保管及任何修改□□，有助于建立信任和可追溯性，尤其是在多方或供□□数据共享□景中。
C. 一种用于□档的大型数据集□□方法
D. 一种□□用于管理 DNS □□的技□
Answer: B (LEAVE A REPLY)
Blockchain or distributed ledger technology can be used to create an immutable, cryptographically verifiable record of data's origin, chain of custody, and any subsequent modifications over time, helping establish trust, transparency, and traceability in scenarios involving data shared or exchanged across multiple parties or organizations, such as supply chain tracking or multi-party data collaboration.

NEW QUESTION: 214

當一個城市的電話由單一交換機連接時，呼叫者只能與總機接線員連接。然後接線員手動連接呼叫。這是哪種類型的網路拓撲的範例？

A. 星號

B. 樹

C. 點對點協定 (PPP)

D. 總線

Answer: (SHOW ANSWER)

The type of network topology that is exemplified by the scenario where telephones in a city are connected by a single exchange, and the caller can only connect with the switchboard operator, who then manually connects the call, is the star topology. A star topology is a type of network topology that consists of a central node, such as a switch, a hub, or a router, that connects to multiple peripheral nodes, such as computers, printers, or phones, using point-to-point links. A star topology allows the communication between the peripheral nodes to be controlled and routed by the central node, which can provide better performance, reliability, and security. A star topology also simplifies the network design, management, and troubleshooting, as the failure or addition of a peripheral node does not affect the rest of the network. A star topology is suitable for the scenario where telephones in a city are connected by a single exchange, and the caller can only connect with the switchboard operator, who then manually connects the call, as it can enable the centralized and efficient communication between the telephones.

NEW QUESTION: 215

某組織開發了一款大型應用程序，該應用程式已通過認證測試。收到評估結果後，該應用程式獲得認證前的最後一步是什麼？

A. 授權官員承擔風險

B. 漏洞修復

C. 採用標準化政策與程序

D. 系統安全計畫(SSP)的批准

Answer: A (LEAVE A REPLY)

The final step before the application can be accredited is the acceptance of risk by the authorizing official, who is responsible for making the final decision on whether to authorize the operation of the system or not. The authorizing official must review the results of the evaluation, the System Security Plan (SSP), and the residual risks, and determine if the risks are acceptable or not.

NEW QUESTION: 216

以下哪□最能描述“脆弱性□估”与“脆弱性□估”之□的区□？

“渗透□□”？

A. 它□是名称不同的相同□程。

B. 漏洞□估旨在□□和□□潜在的弱点，而渗透□□□主□□□利用已□□的漏洞来展示其□□□□境的影响。

C. 渗透□□始□是自□化的，而漏洞□估始□是手□的。

D. 漏洞□估只能在Web□用程序上□行。

Answer: B (LEAVE A REPLY)

A vulnerability assessment systematically identifies, catalogs, and prioritizes known security weaknesses in an environment, typically using automated scanning tools, without attempting exploitation. Penetration testing goes further by actively attempting to exploit identified (and sometimes undiscovered) vulnerabilities to demonstrate the real-world impact and validate whether they can actually be leveraged to compromise systems or data.

NEW QUESTION: 217

下列何者屬於網路入侵偵測技術？

A. 統計異常

B. 周界入侵

C. 連接埠掃描

D. 網路欺騙

Answer: A (LEAVE A REPLY)

Statistical anomaly is a network intrusion detection technique that compares the current network activity with a baseline of normal behavior, and detects any deviations that exceed a predefined threshold. Statistical anomaly can identify unknown or novel attacks, but it may also generate false positives if the baseline is not updated or the threshold is not set properly.

NEW QUESTION: 218

以下哪□最能描述“攻□面”□一□□？

A. 一年内□□某个□□的成功攻□□数

B. 未□授□的用□可能□□向□境中□入数据或从中提取数据的所有点的□和

C. 数据中心的物理□界

D. 系□中已修复漏洞的列表

Answer: B (LEAVE A REPLY)

The attack surface represents the complete set of points of exposure-including network interfaces, open ports, APIs, user inputs, and physical access points-through which an attacker could potentially attempt to gain unauthorized access or exfiltrate data. Reducing the attack surface is a core security design principle.

NEW QUESTION: 219

下列哪一項屬於偵測性存取控制機制？

A. 日誌審□

B. 最小權限原則

C. 密碼複雜度

D. 保密協議

Answer: (SHOW ANSWER)

The access control mechanism that is detective is log review. Log review is a process of examining and analyzing the records or events of the system or network activity, such as user login, file access, or

network traffic, that are stored in log files. Log review can help to detect and identify any unauthorized, abnormal, or malicious access or behavior, and to provide evidence or clues for further investigation or response. Log review is a detective access control mechanism, as it can discover or reveal the occurrence or the source of the security incidents or violations, after they have happened. Least privilege, password complexity, and non-disclosure agreement are not detective access control mechanisms, as they are related to the restriction, protection, or confidentiality of the access or information, not the detection or identification of the security incidents or violations.

NEW QUESTION: 220
某□□□施一□政策，要求由两名不同的□工完成敏感交易，例如一名□工□起□□，另一名□工批准□交易。□属于哪种控制措施？
A. □□分离
B. □□
C. □制休假
D. 双控
Answer: (SHOW ANSWER)
Separation of duties divides critical tasks among multiple individuals so that no single person can complete a sensitive process alone, reducing the risk of fraud or error. (Note: "dual control" is closely related and sometimes used interchangeably, but separation of duties is the broader, standard CISSP term for dividing responsibilities across distinct roles.)

NEW QUESTION: 221
組織 A 將收購組織 B 時收到的大量機密資料記錄新增至其資料儲存。組織 B 的許多使用者和員工不再可用。下列哪一項必須組織 A 0do 來對所取得的資料進行屬性分類和保護？
A. 將組織 A 的資料擁有者指派給所取得的資料。
B. 建立代表組織 B 的前使用者的佔位符帳□。
C. 歸檔引用組織 A 中的使用者的審核記錄。
D. 更改從組織 B 取得的資料的資料分類。
Answer: A (LEAVE A REPLY)
Data ownership is a key concept in data security and classification. Data owners are responsible for defining the value, sensitivity, and classification of the data, as well as the access rights and controls for the data. When Organization A acquires data from Organization B, it should assign data owners from its own organization to the acquired data, so that they can properly classify and secure the data according to Organization A's policies and standards. Creating placeholder accounts, archiving audit records, or changing the data classification are not sufficient or necessary steps to ensure the security of the acquired data.

NEW QUESTION: 222
組織需要遵守支付卡□業資料安全標準 (PCI-DSS)，保護包含持卡人資料的數位和紙本媒體最有效的方法是什麼？

A. 使用並定期更新防毒軟體。
B. 嚴格控制媒體存儲
C. 強制對持卡人資料進行加密。
D. 設定防火牆規則以保護資料。
Answer: C (LEAVE A REPLY)
The most effective approach to safeguard digital and paper media that contains cardholder data is to mandate encryption of cardholder data. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access or modify the data. Encryption protects the confidentiality, integrity, and availability of cardholder data, which is any personally identifiable information associated with a cardholder, such as name, account number, expiration date, or security code. Encryption also helps to comply with the Payment Card Industry Data Security Standard (PCI-DSS), which is a set of requirements and guidelines for ensuring the security of payment card transactions and data. PCI-DSS requires that cardholder data must be encrypted when stored or transmitted over public networks, and that encryption keys must be protected and managed securely. Using and regularly updating antivirus software, maintaining strict control over storage of media, and configuring firewall rules to protect the data are also good practices to safeguard cardholder data, but they are not as effective as encryption, as they may not prevent unauthorized access or modification of the data, or they may not apply to all types of media or scenarios.

NEW QUESTION: 223
以下哪□最能描述“零日”漏洞？
A. 已公开披露并已修复的漏洞
B. 在厂商知□漏洞或□布□丁之前就被利用的漏洞。
C. □在□留系□中□□的漏洞
D. 需要物理接触才能利用的漏洞
Answer: B (LEAVE A REPLY)
A zero-day vulnerability is a previously unknown flaw that is exploited by attackers before the software vendor becomes aware of it and has had the opportunity to develop and release a patch, leaving defenders with "zero days" of preparation time.

NEW QUESTION: 224
限制對計算系統上的檔案系統的存取的最佳方法是什麼？
A. 允許使用者群組限制存取。
B. 使用第三方工具來限制存取。
C. 在每個層級使用最小權限來限制存取。
D. 限制所有使用者的存取。
Answer: C (LEAVE A REPLY)
The principle of least privilege states that every user, process, or system should have the minimum amount of access or privileges necessary to perform their functions, and no more. This principle reduces the attack surface, limits the potential damage of a compromise, and enforces the separation

of duties and responsibilities. Applying the principle of least privilege at each level of the file system, such as directories, files, and permissions, is the best way to restrict access and protect the confidentiality, integrity, and availability of the data. Allowing a user group to restrict access may not be sufficient, as the group may have more privileges than needed, or may not follow the security policies. Using a third-party tool to restrict access may introduce additional risks, such as compatibility issues, vulnerabilities, or malicious code. Restricting access to all users may prevent legitimate access and disrupt the business operations or functions.

NEW QUESTION: 225
下列哪一項是對組織網路執行定期漏洞掃描的主要原因？
A. 提供管理階層漏洞報告。
B. 驗證漏洞修復活動。
C. 防止攻擊者發現漏洞。
D. 修正已知漏洞。
Answer: D (LEAVE A REPLY)
According to the CISSP Official (ISC)2 Practice Tests, the primary reason to perform regular vulnerability scanning of an organization network is to remediate known vulnerabilities. A vulnerability scanning is the process of identifying and measuring the weaknesses and exposures in a system, network, or application, that may be exploited by threats and cause harm to the organization or its assets. A vulnerability scanning can be performed by using various tools, techniques, or methods, such as automated scanners, manual tests, or penetration tests. The primary reason to perform regular vulnerability scanning of an organization network is to remediate known vulnerabilities, which means to fix, mitigate, or eliminate the vulnerabilities that are discovered or reported by the vulnerability scanning. Remediation of known vulnerabilities helps to improve the security posture and effectiveness of the system, network, or application, as well as to reduce the overall risk to an acceptable level.
Providing vulnerability reports to management is not the primary reason to perform regular vulnerability scanning of an organization network, although it may be a benefit or outcome of it. Vulnerability reports are the documents that provide the evidence and analysis of the vulnerability scanning, such as the scope, objectives, methods, results, and recommendations of the vulnerability scanning. Vulnerability reports help to communicate and document the findings and issues of the vulnerability scanning, as well as to support the decision making and planning for the remediation of the vulnerabilities. Validating vulnerability remediation activities is not the primary reason to perform regular vulnerability scanning of an organization network, although it may be a part or step of it. Validating vulnerability remediation activities is the process of verifying and testing the effectiveness and completeness of the remediation actions that are taken to address the vulnerabilities, such as patching, updating, configuring, or replacing the system, network, or application components. Validating vulnerability remediation activities helps to ensure that the vulnerabilities are properly and successfully remediated, and that no new or residual vulnerabilities are introduced or left behind. Preventing attackers from discovering vulnerabilities is not the primary reason to perform regular vulnerability scanning of an organization network, although it may be a benefit or outcome of it. Preventing attackers from discovering vulnerabilities is the process of hiding or obscuring the vulnerabilities from the

potential attackers, by using various techniques or methods, such as encryption, obfuscation, or deception. Preventing attackers from discovering vulnerabilities helps to reduce the likelihood and opportunity of the attackers to exploit the vulnerabilities, but it does not address the root cause or the impact of the vulnerabilities.

NEW QUESTION: 226
在聯合身分管理（FIM）中，下列哪一項代表了聯合的概念？
A. 邏輯上分組為單一實體的資訊集合
B. 收集、維護和停用一個或多個系統、目錄或應用程式中的使用者物件和屬性
C. 系統中通用身份資訊的集合
D. 彼此之間建立信任的域的集合
Answer: D (LEAVE A REPLY)
The concept of federation in Federated Identity Management (FIM) is the collection of domains that have established trust among themselves. A domain is a logical or administrative boundary that defines the scope and authority of an identity provider (IdP) or a service provider (SP). An IdP is an entity that creates, maintains, and verifies the identities and attributes of the users. An SP is an entity that provides services or resources to the users, and relies on the IdP for the authentication and authorization of the users. A federation is a group of domains that have agreed to share and accept the identities and attributes of the users across the domains, based on a common set of policies, standards, and protocols. A federation enables the users to access multiple services or resources from different domains, using a single or federated identity, without having to create or manage multiple accounts or credentials. A federation also enhances the security, privacy, and convenience of the users and the domains, by reducing the identity management overhead and complexity, and by enabling the users to control the disclosure and use of their identity information.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 227
開發資訊安全管理系統時首先考慮下列何者？
A. 確定適用於組織的合約安全義務
B. 了解資訊資□的價□
C. 決定管理階層可以容忍的殘餘風險水平
D. 確定相關的立法和監管合規要求
Answer: (SHOW ANSWER)

When developing an information security management system (ISMS), an initial consideration is to understand the value of the information assets that the organization owns or processes. An information asset is any data, information, or knowledge that has value to the organization and supports its mission, objectives, and operations. Understanding the value of the information assets helps to determine the appropriate level of protection and investment for them, as well as the potential impact and consequences of losing, compromising, or disclosing them.
Understanding the value of the information assets also helps to identify the stakeholders, owners, and custodians of the information assets, and their roles and responsibilities in the ISMS.

NEW QUESTION: 228
下列哪些是災難復原計畫 (DRP) 的全部要素？
A. 記錄 ORP 的實際位置，制定事件通知程序，評估關鍵組件的成本
B. 記錄 ORP 的實際位置，制定事件通知程序，建立復原位置
C. 維護所有伺服器日誌的正確記錄，制定事件通知程序，建立復原位置
D. 記錄 ORP 的實際位置，記錄所有ORP 計畫會議的分鐘數，建立恢復位置
Answer: B (LEAVE A REPLY)
The elements of a disaster recovery plan (DRP) are document the actual location of the ORP, developing an incident notification procedure, and establishing recovery locations. A DRP is a plan that defines the procedures and resources for restoring the critical business functions and systems after a disaster or an outage. A DRP should include the following elements:
Document the actual location of the ORP: The ORP is the operational recovery plan, which is a plan that defines the procedures and resources for restoring the operational functions and systems after a disaster or an outage. The ORP should be documented and stored in a secure and accessible location, such as a cloud storage service, a remote data center, or a fireproof safe, and it should be updated and reviewed regularly. The actual location of the ORP should be documented in the DRP, so that the relevant stakeholders, such as the management, the staff, or the vendors, can access and execute the ORP in the event of a disaster or an outage.
Developing an incident notification procedure: The incident notification procedure is a procedure that defines the roles, responsibilities, and actions of the stakeholders involved in the disaster recovery process, and the methods and channels of communication and information exchange among them. The incident notification procedure should be developed and documented in the DRP, and it should include the following information:
The incident response team, which is the group of people who are responsible for initiating, coordinating, and managing the disaster recovery process, and who have the authority and the skills to make decisions and take actions.
The incident escalation process, which is the process of notifying and involving the higher-level or external stakeholders, such as the management, the customers, or the authorities, about the occurrence and the details of the disaster or the outage, and seeking their approval, support, or guidance.
The incident communication plan, which is the plan that defines the methods and channels of communication and information exchange among the stakeholders, such as the phone, the email, or

the social media, and the frequency and the content of the communication and information, such as the status, the impact, or the resolution of the disaster or the outage.
Establishing recovery locations: The recovery locations are the alternative sites or facilities where the organization can resume its critical business functions and systems after a disaster or an outage. The recovery locations should be established and documented in the DRP, and they should include the following information:
The type and the level of the recovery locations, such as the hot site, which is a fully equipped and operational site that can provide immediate recovery, the warm site, which is a partially equipped and operational site that can provide rapid recovery, or the cold site, which is a basic and non-operational site that can provide delayed recovery.
The location and the distance of the recovery locations, such as the local, which is within the same city or region as the primary site, the regional, which is within the same country or continent as the primary site, or the global, which is in a different country or continent than the primary site.

NEW QUESTION: 229
在檢視安全測試結果時設定期望時，向審口者傳達下列哪一項敘述最重要？
A. 目標的安全狀況不能進一步受到損害。
B. 測試結果代表對目標的時間點評估。
C. 如果目標得到適當的強化，測試結果的準確性可以大大提高。
D. 發現的缺陷可以立即修正
Answer: (SHOW ANSWER)
The most important statement to convey to reviewers when setting expectations for reviewing the results of a security test is that the results of the tests represent a point-in-time assessment of the target(s). A security test is a process of evaluating and measuring the security posture and performance of an information system or a network, by using various tools, techniques, and methods, such as vulnerability scanning, penetration testing, or security auditing. The results of a security test reflect the security state of the target(s) at the time of the test, and they may not be valid or accurate for a different time period, as the security environment and conditions may change due to various factors, such as new threats, patches, updates, or configurations.
Therefore, reviewers should understand that the results of a security test are not definitive or permanent, but rather indicative or temporary, and that they should be interpreted and used accordingly. The statement that the target's security posture cannot be further compromised is not true, as a security test does not guarantee or ensure the security of the target(s), but rather identifies and reports the security issues or weaknesses that may exist. The statement that the accuracy of testing results can be greatly improved if the target(s) are properly hardened is not relevant, as a security test is not meant to improve the accuracy of the results, but rather to assess the security of the target(s), and hardening the target(s) before the test may not reflect the actual or realistic security posture of the target(s). The statement that the deficiencies identified can be corrected immediately is not realistic, as a security test may identify various types of deficiencies that may require different levels of effort, time, and resources to correct, and some deficiencies may not be correctable at all, due to technical, operational, or financial constraints.

NEW QUESTION: 230
以下哪□最能描述“出口点网□□□控制(NAC)”的目的？
A. □根据内容□□控制出站互□网流量
B. 在授予□□网□□□□限之前，□制□行安全策略，□估□□的身份健康状况和合□性，并在之后持□□控合□性。
C. 一款□□用于管理无□接入点信号□度的工具
D. 一种加密局域网所有流量的方法
Answer: B (LEAVE A REPLY)
Network Access Control enforces security policies that evaluate a connecting device's identity, security posture (such as patch level, antivirus status, and configuration compliance) before granting network access, and can continuously monitor compliance thereafter, potentially quarantining or restricting non-compliant devices to a remediation network segment.

NEW QUESTION: 231
在目標主機上，下列哪一個OSI 模型層會丟棄 UDP 標頭中校驗和錯誤的段？
A. 網絡
B. 數據鏈接
C. 運輸
D. 會話
Answer: C (LEAVE A REPLY)
The transport layer is the OSI model layer that will discard a segment with a bad checksum in the UDP header. The transport layer is responsible for providing end-to-end data transmission and reliability between the source and destination hosts. The transport layer uses protocols such as TCP (transmission control protocol) or UDP (user datagram protocol) to segment, encapsulate, and deliver the data. The transport layer also performs error detection and correction using checksums, which are values calculated from the data and added to the header of each segment.
The checksums are verified at the destination host to ensure the integrity of the data. If the checksum in the UDP header does not match the expected value, the transport layer will discard the segment as corrupted.

NEW QUESTION: 232
邏輯存取控制的前兩個組成部分是什麼？
A. 保密與身分驗證
B. 認證與識別
C. 身分識別與保密性
D. 身份驗證和可用性
Answer: B (LEAVE A REPLY)
Authentication and identification are the first two components of logical access control, which is the process of granting or denying access to resources based on the identity and credentials of a user or a device. Identification is the process of verifying the identity of a user or a device, such as by using a

username, an email address, or a certificate. Authentication is the process of verifying the validity of the credentials of a user or a device, such as by using a password, a token, or a biometric factor. Confidentiality and availability are not components of logical access control, but rather properties or objectives of information security. Confidentiality is the property of preventing unauthorized disclosure of information, while availability is the property of ensuring timely and reliable access to information.

NEW QUESTION: 233
雲端服務接受使用者發出的安全性斷言標記語言 (SAML) 斷言，但攻擊者能□欺騙網路上的註冊帳□並□詢 SAML 提供者。
針對此缺陷最常見的攻擊手段是什麼？
A. 攻擊者偽造以不同使用者身分進行驗證的請求。
B. 攻擊者利用 SAML 斷言在安全性網域上註冊帳□。
C. 攻擊者透過重複驗證同一使用者的身份，對安全域實施拒□服務(DoS)。
D. 攻擊者在安全域之間交換認證和授權資料。
Answer: (SHOW ANSWER)
The most common attack leveraged against this flaw is that the attacker forges requests to authenticate as a different user. SAML is a standard that enables the exchange of authentication and authorization data between different security domains, such as a service provider and an identity provider. SAML uses XML-based messages, called assertions, to convey the information about the identity, attributes, and entitlements of a user. SAML enables single sign-on (SSO), which is a feature that allows a user to access multiple services or applications with a single login session. A flaw in the SAML implementation or configuration could allow an attacker to spoof a registered account on the network and query the SAML provider. The most common attack leveraged against this flaw is that the attacker forges requests to authenticate as a different user, by manipulating or tampering with the SAML assertions. For example, the attacker could modify the user identifier, the timestamp, the signature, or the encryption of the SAML assertion, and use it to impersonate or access another user's account or privileges. This attack could compromise the security and integrity of the SAML-based SSO system, and allow the attacker to access the sensitive or confidential data or resources of the service provider or the identity provider.

NEW QUESTION: 234
某組織聘請顧問對其□部安全控制進行系統組織控制 (SOC) 2 審計。審計員記錄了一項與應用程式介面 (API) 相關的發現，該API 執行的操作與系統的範圍或目標不符。在這種情況下，哪項信任服務原則最適用？
A. 處理完整性
B. 可用性
C. 保密性
D. 安全
Answer: (SHOW ANSWER)

Processing integrity is one of the five trust service principles that are used to evaluate the security controls of a service organization in a SOC 2 audit. Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of the system's processing of data and transactions. An API that performs an action that is not aligned with the scope or objective of the system violates the processing integrity principle, because it may compromise the quality, reliability, and consistency of the system's output. The other trust service principles are availability, confidentiality, security, and privacy.

NEW QUESTION: 235
功能安全測試在系統開發生命週期（SDLC）的哪個階段最為重要？
A. 操作/維護
B. 實施
C. 收購/開發
D. 口動
Answer: C (LEAVE A REPLY)
Functional security testing is most critical during the acquisition / development phase of the system development life cycle (SDLC). Functional security testing is a type of software testing that verifies that the system meets the functional security requirements and specifications, such as authentication, authorization, encryption, logging, and error handling. Functional security testing can help identify and correct any security flaws or vulnerabilities in the system before it is deployed or released. The acquisition / development phase is the phase where the system is designed, coded, tested, and integrated. This is the phase where functional security testing should be performed as part of the quality assurance and security assurance processes, and where security should be built into the system from the start, following the principle of secure by design.

NEW QUESTION: 236
下列哪一項口動災難復原計畫的系統復原階段？
A. 疏散災難現場
B. 評估災難後的損失程度
C. 發布正式災難聲明
D. 口動組織的熱點站點
Answer: (SHOW ANSWER)
Activating the organization's hot site initiates the system recovery phase of a disaster recovery plan. A disaster recovery plan (DRP) is a document that describes the procedures and actions to be taken before, during, and after a disaster that affects the IT systems and operations of an organization. A DRP typically consists of four phases: prevention, preparation, response, and recovery. The system recovery phase is the phase where the organization restores the IT systems and operations to a normal or near-normal state, using the backup data and resources that were stored or deployed at an alternate site. A hot site is a type of alternate site that is fully equipped and ready to resume the IT systems and operations of the organization within a short time, usually minutes or hours, after a disaster. A hot site has the hardware, software, network, power, and security components that match or mirror the primary site of the organization.

Activating the organization's hot site means switching the IT systems and operations from the primary site to the hot site, and ensuring that the hot site can support the business continuity and recovery objectives of the organization. Evacuating the disaster site, assessing the extent of damage following the disaster, and issuing a formal disaster declaration are actions that belong to the response phase, not the recovery phase, of a DRP.

NEW QUESTION: 237
使用者發送電子郵件請求，請求對不被視為敏感的文件進行唯讀存取。自主存取控制 (DAC) 方法已經到位。管理員應該採取哪一種最適合的方法？
A. 管理員應請求資料擁有者批准使用者存取權限
B. 管理員應請求經理批准使用者存取權限
C. 管理員應直接授予對非敏感檔案的存取權限
D. 管理員應評估使用者存取需求並授予或拒口存取權限
Answer: (SHOW ANSWER)
According to the CISSP Official (ISC)2 Practice Tests3, the most suitable approach that the administrator should take when a user requests read-only access to files that are not considered sensitive in a Discretionary Access Control (DAC) methodology is to request data owner approval to the user access. DAC is a type of access control that grants or denies access to an object based on the identity and permissions of the subject, and the discretion of the owner of the object. The owner of the object has the authority and responsibility to determine who can access the object and what level of access they can have, such as read, write, execute, or delete. The owner can also delegate the access rights to other subjects or groups, or revoke them as needed.
The administrator is the person who manages and maintains the system and the access control mechanisms, but does not have the authority to grant or deny access to the objects without the owner's consent. Therefore, the administrator should request data owner approval to the user access, regardless of the sensitivity of the files, to ensure that the access is authorized and compliant with the DAC methodology. Requesting manager approval for the user access is not the most suitable approach, as the manager may not be the owner of the files, and may not have the authority or knowledge to grant or deny access to the files. Directly granting the access to the non-sensitive files is not the most suitable approach, as it may violate the DAC methodology and the owner's discretion, and may introduce unauthorized or excessive access to the files.
Assessing the user access need and either granting or denying the access is not the most suitable approach, as it may violate the DAC methodology and the owner's discretion, and may introduce unauthorized or excessive access to the files.

NEW QUESTION: 238
下列哪一項是聯合身分識別管理 (FIM) 實施模型的主要組成部分，用於在數十個組織之間建立網路？
A. 身分即服務 (IDaaS)
B. 基於屬性的存取控制 (ABAC)
C. 交叉認證
D. 可信任第三方 (TTP)

Answer: C (LEAVE A REPLY)
Cross-certification is a major component of the federated identity management (FIM) implementation model and is used to establish a network between dozens of organizations.
Cross-certification allows two different organizations to establish mutual trust by exchanging and validating each other's digital certificates. This mutual trust enables users in one organization to access resources in another organization without the need for separate user accounts or authentication processes.

NEW QUESTION: 239
使用者透過連接通用序列匯流排 (USB) 儲存裝置使電腦感染了惡意軟體。下列哪一項對於減輕未來感染最有效？
A. 制定書面組織政策，禁止未經授權的USB 設備
B. 訓練使用者了解在 USB 裝置中傳輸資料的危險
C. 實現USB埠連接的集中技術控制
D. 加密包含靜態資料的可移動 USB 設備
Answer: C (LEAVE A REPLY)
The most effective way to mitigate future infections from USB devices is to implement centralized technical control of USB port connections. This means controlling whether USB ports can be used on devices at all and restricting or managing which USB devices can be connected to computers. This can be achieved through the following measures:
Disabling USB ports entirely, or for non-authorized users, on machines where USB connections are not needed.
Using endpoint security solutions that restrict or monitor USB access, ensuring only approved devices can be used.
Implementing whitelisting software that only allows specific, authorized USB devices to connect.
By centrally controlling USB port access, you can prevent the risk of future malware infections that may occur from connecting unauthorized or infected USB devices.

NEW QUESTION: 240
下列哪一項□動災難復原計畫的系統復原階段？
A. 發布正式災難聲明
B. □動組織的熱點站點
C. 疏散災難現場
D. 評估災難後的損失程度
Answer: B (LEAVE A REPLY)
The systems recovery phase of a disaster recovery plan is the phase that involves restoring the critical systems and operations of the organization after a disaster. The systems recovery phase is initiated by activating the organization's hot site. A hot site is a fully equipped and operational alternative site that can be used to resume the business functions within a short time after a disaster. A hot site typically has the same hardware, software, network, and data as the original site, and can be switched to quickly

and seamlessly. A hot site can ensure the continuity and availability of the organization's systems and services during a disaster recovery situation.

NEW QUESTION: 241
以下哪□最能描述“网□威□□因”？
A. □法医□□□程中收集的□据□行加密的□程
B. □□特定网□攻□的□任人(个人、□体或国家)的□程，通常基于技□指□ □□、技□和程序(TTP)以及情境情□。
C. 基于敏感性□数据□行分□的□程
D. 一种□算攻□造成的□□影响的方法
Answer: B (LEAVE A REPLY)
Cyber threat attribution is the analytical process of identifying the specific individual, group, or nation-state responsible for a cyberattack, typically based on a combination of technical indicators, observed tactics/techniques/procedures (TTPs), malware characteristics, infrastructure overlap, and broader contextual or geopolitical intelligence, though attribution can be challenging and is often assigned with varying degrees of confidence.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 242
下列哪一項是安全性修補程式管理流程中最關鍵的成功因素？
A. 追蹤與報告庫存
B. 支援文檔
C. 報告的管理審□
D. 風險與影響分析
Answer: (SHOW ANSWER)
Security patch management is a process of identifying, acquiring, testing, deploying, and verifying patches or updates for software systems or applications to fix security vulnerabilities or bugs. The most critical success factor in the security patch management process is to perform a risk and impact analysis before applying any patches or updates. A risk and impact analysis helps to evaluate the severity and urgency of the patch or update, the potential threats and consequences of not applying the patch or update, and the possible side effects or disruptions of applying the patch or update. A risk and impact analysis can help to prioritize, plan, and implement the patch or update in a timely and effective manner, while minimizing the risks and impacts to the system or application. Tracking and reporting on

inventory, supporting documentation, and management review of reports are also important factors in the security patch management process, but they are not as critical as the risk and impact analysis.

NEW QUESTION: 243
為什麼要建立一個系統來將不同類別的資訊彼此隔離並按使用者權限將它們分開？
A. 組織可以在發生訴訟時避免電子取證流程。
B. 組織的基礎設施安排清晰，職責範圍簡化。
C. 組織可以改變其係統政策以遵守相互衝突的國家法律。
D. 組織需要向各種第三方組織提供不同的服務。
Answer: C (LEAVE A REPLY)
A system that is structured to isolate different classes of information from one another and segregate them by user jurisdiction can help the organization to vary its system policies to comply with conflicting national laws. Different classes of information may have different levels of sensitivity, confidentiality, or classification, and may require different security measures and controls to protect them. Different user jurisdictions may have different legal or regulatory requirements, standards, or expectations for the information, and may impose different obligations or restrictions on the organization. By isolating and segregating the information by class and jurisdiction, the organization can tailor its system policies to meet the specific needs and demands of each class and jurisdiction, and avoid any conflicts or violations of the national laws.

NEW QUESTION: 244
組織將執行哪種類型的測試來定位和瞄準可利用的缺陷？
A. 穿透
B. 系統
C. 效能
D. 漏洞
Answer: (SHOW ANSWER)
Penetration testing is a type of test that an organization performs in order to locate and target exploitable defects in its information systems and networks. Penetration testing simulates a real- world attack scenario, where a tester, also known as a penetration tester or ethical hacker, tries to find and exploit the vulnerabilities in the system or network, using the same tools and techniques as a malicious attacker. The goal of penetration testing is to identify the weaknesses and gaps in the security posture of the organization, and to provide recommendations and solutions to mitigate or eliminate them. Penetration testing can help the organization improve its security awareness, compliance, and resilience, and prevent potential breaches or incidents.

NEW QUESTION: 245
對系統日誌伺服器的拒口服務 (DoS) 攻擊利用了下列哪種協定的弱點？
A. 點對點協定 (PPP) 與網際網路控制訊息協定 (ICMP)
B. 傳輸控制協定 (TCP) 與使用者資料封包協定 (UDP)

C. 位址解析協定 (ARP) 和反向位址解析協定 (RARP)
D. 傳輸層安全性 (TLS) 和安全通訊端層 (SSL)
Answer: B (LEAVE A REPLY)
A DoS attack on a syslog server exploits weakness in TCP and UDP protocols. A syslog server is a server that collects and stores log messages from various devices on a network, such as routers, switches, firewalls, or servers. A syslog server uses either TCP or UDP protocols to receive log messages from the devices. A DoS attack on a syslog server can exploit the weakness of these protocols by sending a large volume of fake or malformed log messages to the syslog server, causing it to crash or become unresponsive. The other protocols are not relevant to a syslog server or a DoS attack.

NEW QUESTION: 246
攻擊者最有可能瞄準下列哪一項來獲得系統的特權存取？
A. 寫入系統資源的程式
B. 寫入使用者目錄的程式
C. 包含敏感資訊的日誌文件
D. 包含系統呼叫的日誌文件
Answer: A (LEAVE A REPLY)
An attacker is most likely to target programs that write to system resources to gain privileged access to a system. System resources are the hardware and software components that are essential for the operation and functionality of a system, such as the CPU, memory, disk, network, operating system, drivers, libraries, etc. Programs that write to system resources may have higher privileges or permissions than programs that write to user directories or log files. An attacker may exploit vulnerabilities or flaws in these programs to execute malicious code, escalate privileges, or bypass security controls. Programs that write to user directories or log files are less likely to be targeted by an attacker, as they may have lower privileges or permissions, and may not contain sensitive information or system calls. User directories are the folders or locations where users store their personal files or data. Log files are the records of events or activities that occur in a system or application.

NEW QUESTION: 247
使用名為 Mirai 的惡意軟體進行分散式阻斷服務 (DDoS) 攻擊，建立大規模命令和控制系統來□動殭屍網路。下列哪些設備是用來□生攻擊流量的主要來源？
A. 物聯網 (IoT) 設備
B. Microsoft Windows 主機
C. 執行開源作業系統 (OS) 的 Web 伺服器
D. 運行 Android 的行動裝置
Answer: (SHOW ANSWER)
The primary sources used to generate the attack traffic in the DDoS attack using Mirai malware were IoT devices. A DDoS attack is a type of attack that aims to disrupt or degrade the availability or performance of a system or a service, by overwhelming or flooding it with a large amount of traffic or requests from multiple sources. A DDoS attack can cause the system or service to slow down, crash,

or become inaccessible for the legitimate users or customers. Mirai is a malware that infects and hijacks IoT devices, such as cameras, routers, or printers, and turns them into a botnet, which is a network of compromised devices that are controlled by a central command and control server. Mirai malware scans the internet for vulnerable IoT devices that use default or weak credentials, and infects them with malicious code that allows the attacker to remotely control them. Mirai malware was used to launch a massive DDoS attack in 2016, targeting several high-profile websites and services, such as Twitter, Netflix, or Amazon, and causing widespread internet disruption. IoT devices were the primary sources used to generate the attack traffic in the DDoS attack using Mirai malware, because:
They are abundant and ubiquitous, as there are billions of IoT devices connected to the internet, and they are expected to grow exponentially in the future.
They are insecure and vulnerable, as many IoT devices lack proper security measures, such as encryption, authentication, or patching, and use default or weak credentials, such as admin or 1234, that can be easily guessed or brute-forced by the attackers.
They are powerful and capable, as many IoT devices have sufficient processing power, memory, and bandwidth to generate a large amount of traffic or requests, and can use various protocols, such as HTTP, TCP, or UDP, to target different layers of the network stack.

NEW QUESTION: 248
以下哪□最能描述物理或网□安全控制中的“故障安全”□□与“故障开放”□□？
A. 故障安全模式默□允□所有□□，而故障开放模式默□拒□所有□□。
B. 故障安全模式默□在□生故障□拒□□□(□先考□安全性)，而故障开放模式默□在□生故障□允□□□(□先考□可用性或安全性)。
C. 故障安全与故障开放是相同的概念，只是名称不同。
D. □两个□□均□□用于加密密□管理。
Answer: B (LEAVE A REPLY)
Fail-secure design ensures that a control defaults to a denied or locked state upon failure, prioritizing security over availability (e.g., a door that stays locked if power fails). Fail-open design ensures that a control defaults to an allowed or unlocked state upon failure, prioritizing availability or life safety (e.g., a fire door unlocking automatically during a power outage to allow evacuation).
The appropriate choice depends on the specific risk context, including life-safety considerations.

NEW QUESTION: 249
傳輸層安全性 (TLS) 中使用的數位憑證支援下列哪一項？
A. 資訊輸入驗證
B. 不可否認控制與資料加密
C. 多重驗證 (MFA)
D. 伺服器身分與資料保密
Answer: B (LEAVE A REPLY)
Digital certificates are electronic documents that contain the public key of an entity and are signed by a trusted third party, called a Certificate Authority (CA). Digital certificates are used in Transport Layer

Security (TLS), a protocol that provides secure communication over the Internet, by enabling the following functions:
Server identity: The client can verify the identity of the server by checking the validity of its digital certificate and the signature of the CA.
Data confidentiality: The client and the server can use the public keys in their digital certificates to establish a symmetric key for encrypting the data exchanged between them.
Non-repudiation controls: The client and the server can use their private keys to digitally sign the data they send, which provides proof of origin and integrity of the data, and prevents the sender from denying the transmission.

NEW QUESTION: 250
下列哪一個安全測試策略最適合安全成熟度較低到中等的公司？
A. 負載測試
B. 白盒測試
C. 黑盒測試
D. 效能測試
Answer: (SHOW ANSWER)
Black-box testing is a security testing strategy that simulates an external attack on a system or application, without any prior knowledge of its internal structure, design, or implementation. Black- box testing is best suited for companies with low to moderate security maturity, as it can reveal the most obvious and common vulnerabilities, such as misconfigurations, default credentials, or unpatched software. Black-box testing can also provide a realistic assessment of the system's security posture from an attacker's perspective.

NEW QUESTION: 251
資訊科技 (IT) 專業人員參加有關當前事件回應方法的網路安全研討會。
遵守哪些道德準則？
A. 為委託人提供勤勉、稱職的服務
B. 保護社會、聯邦和基礎設施
C. 促進和保護職業
D. 行為誠實、公正、負責、合法
Answer: C (LEAVE A REPLY)
Attending a cybersecurity seminar to learn about current incident response methodologies aligns with the ethical canon of advancing and protecting the profession. It involves enhancing one's knowledge and skills, contributing to the growth and integrity of the field, and staying abreast of the latest developments and best practices in information security.

NEW QUESTION: 252
組織中誰負責資料資訊資口的分類？
A. 資料擁有者

B. 資料架構師
C. 首席資訊安全長 (CISO)
D. 資訊長 (CIO)
Answer: A (LEAVE A REPLY)
The person in the organization who is accountable for the classification of data information assets is the data owner. The data owner is the person or entity that has the authority and responsibility for the creation, collection, processing, and disposal of a set of data. The data owner is also responsible for defining the purpose, value, and classification of the data, as well as the security requirements and controls for the data. The data owner should be able to determine the impact of the data on the mission of the organization, which means assessing the potential consequences of losing, compromising, or disclosing the data. The impact of the data on the mission of the organization is one of the main criteria for data classification, which helps to establish the appropriate level of protection and handling for the data. The data owner should also ensure that the data is properly labeled, stored, accessed, shared, and destroyed according to the data classification policy and procedures.

NEW QUESTION: 253
開發一個系統，使其業務使用者可以執行業務功能，但不能執行使用者管理功能應用程式管理員可以執行管理功能，但不能執行使用者業務功能。這些功能最好描述為：
A. 最小權限原則。
B. 基於規則的存取控制。
C. 強制存取控制(MAC)。
D. 職責分離。
Answer: (SHOW ANSWER)
The capabilities of the system that allow its business users to perform business functions but not user administration functions, and its application administrators to perform administration functions but not user business functions, are best described as separation of duties. Separation of duties is a security principle that divides the roles and responsibilities of different tasks or functions among different individuals or groups, so that no one person or group has complete control or authority over a critical process or asset. Separation of duties can help to prevent fraud, collusion, abuse, or errors, and to ensure accountability, oversight, and checks and balances.
Least privilege, rule based access controls, and Mandatory Access Control (MAC) are not the best descriptions of the capabilities of the system, as they do not reflect the division of roles and responsibilities among different users or groups.

NEW QUESTION: 254
無線用□報告網路連線時斷時續。當使用者中斷連線並重新連線時，每次都會利用Web 驗證程序來恢復連線。網路管理員可以隨時□看連接到AP的設備。下列哪一個步驟最可能確定問題的原因？
A. 驗證強制門□設定上的會話逾時配置
B. 檢□客□端無線設定上的加密協定是否不符。
C. 確認 Web 驗證期間使用了有效的密碼。

D. 調口由邪惡孿生 AP 導致的客口端解除關聯

Answer: A (LEAVE A REPLY)

The most likely step to determine the cause of the issue is to verify the session time-out configuration on the captive portal settings. A captive portal is a web page that requires the user to authenticate or accept some terms of service before accessing the Internet through a wireless network. A session time-out is a parameter that defines how long the user can stay connected to the network without re-authenticating or re-accepting the terms of service. If the session time-out is set too low, the user may experience intermittent Internet connectivity, as they will have to disconnect and reconnect frequently, using the web authentication process each time. The network administrator can check the session time-out configuration on the captive portal settings and adjust it accordingly to prevent or reduce the issue.

NEW QUESTION: 255

為什麼在低風險環境中使用套件過濾路由器？

A. 它們是高解析度來源辨別和辨識工具。

B. 它們快速且靈活，並且可以防止網際網路通訊協定(IP) 欺騙。

C. 它們快速、靈活且透明。

D. 它們強制執行強大的使用者驗證和審核 tog 生成。

Answer: C (LEAVE A REPLY)

Packet filtering routers are used in low-risk environments because they offer speed, flexibility, and transparency in filtering traffic based on IP protocol, source/destination IP address, or port number without adding significant overhead or complexity.

NEW QUESTION: 256

一家公司聘請了一位安全顧問來建立其漏洞管理計劃。該顧問目前正處於部署階段。下列哪一項任務屬於此流程的一部分？

A. 選擇並購買支援技術。

B. 確定該計劃的預算和成本分析。

C. 衡量該計劃既定目標的有效性。

D. 教育和培訓主要利害關係人。

Answer: (SHOW ANSWER)

Selecting and procuring supporting technologies is a task that is part of the deployment phase of establishing a vulnerability management program. A vulnerability management program is a systematic and proactive approach to identifying, assessing, and mitigating the vulnerabilities that may affect the organization's information systems and assets. A vulnerability management program consists of several phases, such as planning, design, deployment, operation, and improvement. The deployment phase is the phase where the vulnerability management program is implemented and executed, using the resources and the technologies that are required to support the program. One of the tasks in the deployment phase is to select and procure the supporting technologies, such as the tools, the software, the hardware, and the services that are needed to perform the vulnerability scanning, the vulnerability

analysis, the vulnerability reporting, and the vulnerability remediation. Selecting and procuring the supporting technologies can help ensure that the vulnerability management program is effective, efficient, and reliable, and that it meets the organization's security and business objectives.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 257
在取證資料分析階段執行下列哪些步驟？
A. 收集已知的系統文件
B. 搜尋相關字串。
C. 建立文件列表
D. 恢復已刪除的資料。
Answer: B (LEAVE A REPLY)
Searching for relevant strings is one of the steps performed during the forensic data analysis phase. Strings are sequences of printable characters that may contain useful information, such as passwords, usernames, email addresses, file names, and commands. Searching for strings can help to identify and extract evidence from the data collected during the forensic acquisition phase.
Collecting known system files, creating file lists, and recovering deleted data are steps performed during the forensic acquisition phase, not the forensic data analysis phase. The forensic acquisition phase involves creating a bit-by-bit copy of the original data source, verifying its integrity, and preserving its chain of custody. The forensic data analysis phase involves examining and interpreting the data to find relevant facts and artifacts that support the investigation.

NEW QUESTION: 258
使用什麼技術來欺騙電子郵件的來源可以成功隱藏寄件者的網際網路通訊協定 (IP) 位址？
A. 更改回覆數據
B. 網頁抓取
C. 洋蔥路由
D. 虛擬私人網路 (VPN)
Answer: (SHOW ANSWER)
Email spoofing is a technique used to forge the origin of an email by altering the header fields, such as the sender's address, name, or reply-to address. Email spoofing can be used for malicious purposes, such as phishing, spamming, or impersonating someone else. One technique used for spoofing the origin of an email that can successfully conceal the sender's Internet Protocol (IP) address is onion routing. Onion routing is a method of anonymous communication that encrypts and routes the

messages through multiple layers of intermediate nodes, called onion routers, before reaching the final destination. Each onion router only knows the previous and next hop of the message, but not the entire route or the origin and destination of the message. This way, the sender's IP address is hidden from the recipient and any eavesdroppers. Therefore, the correct answer is C.

NEW QUESTION: 259
作為安全評估計劃的一部分，安全專業人員被要求在新網站上使用負面測試策略。將執行下列哪項操作？
A. 使用網路掃描器掃描網站□的漏洞。
B. 執行程式碼審□以確保正確處理資料庫參考。
C. 建立與 Web 伺服器的安全連接，以驗證是否僅開放核准的連接埠。
D. 在網路表單中僅輸入數字，並驗證網站是否提示使用者輸入有效的□容。
Answer: (SHOW ANSWER)
Negative testing focuses on testing a system by inputting data or performing actions that are invalid, unexpected, or erroneous, to see how the system behaves. The goal is to verify that the system handles these invalid inputs appropriately, either by providing an appropriate error message or by rejecting the input.
Option D: Entering only numbers in the web form when the field expects a different type of input (e.g., letters, special characters) is a classic negative testing approach. In this case, you would expect the website to prompt the user to enter valid input (such as an error message or validation prompt). This helps ensure that the form is properly validating user inputs and not accepting inappropriate or potentially harmful data.

NEW QUESTION: 260
下列哪一個是身分和存取配置生命週期的最後階段？
A. 重新認證
B. 撤銷
C. 刪除
D. 驗證
Answer: (SHOW ANSWER)
Revocation is the final phase of the identity and access provisioning lifecycle. The identity and access provisioning lifecycle is the set of activities and stages that govern the creation, modification, and deletion of user accounts and access privileges in an organization. The identity and access provisioning lifecycle consists of six phases: request, approval, provision, test, review, and audit. Revocation is the process of terminating or disabling the user accounts and access privileges when they are no longer needed, used, or authorized, such as when a user leaves the organization, changes roles, or violates the policies. Revocation can be done manually or automatically, depending on the triggers and the mechanisms used. Revocation ensures that the user accounts and access privileges are removed in a timely and secure manner, and that the principle of least privilege and the separation of duties are maintained.

NEW QUESTION: 261
下列哪一項是有關身份驗證的最重要的操作？
A. 授予存取權限
B. 正在系統中註冊
C. 建立審核控制
D. 取得行政授權
Answer: B (LEAVE A REPLY)
The most important action regarding authentication is enrolling in the system. Authentication is the process of verifying the identity or attributes of a user, device, or process that requests access to a system or resource. Authentication can be based on something the user knows, such as a password or a PIN; something the user has, such as a smart card or a token; something the user is, such as a fingerprint or a face; or something the user does, such as a signature or a voice. Enrolling in the system is the first and essential step of authentication, as it establishes the identity or attributes of the user and associates them with a unique identifier, such as a username or an account number. Enrolling in the system also involves creating and storing the authentication factors, such as passwords, tokens, or biometrics, that will be used to authenticate the user in the future. Without enrolling in the system, authentication cannot take place. Granting access rights, establishing audit controls, and obtaining executive authorization are not actions regarding authentication, but rather actions regarding authorization, accountability, and governance, respectively. Authorization is the process of granting or denying access to a system or resource based on the authenticated identity or attributes of the user. Accountability is the process of holding users responsible for their actions and activities on a system or resource.
Governance is the process of defining and implementing the policies, procedures, and standards for managing and securing a system or resource.

NEW QUESTION: 262
請參考以下資訊回答問題。
為確保安全，公司對桌上型電腦進行了資料清除，以便在同等安全環境下重新使用資料已依照公司政策銷毀，所有標記和其他顯示資料敏感度的外部標識(原先儲存在磁頭驅動器上)均已移除。
磁驅動器依照口品製造商的口明進行兩次消磁後，消磁最可能的安全性問題是什麼？
A. 商業口品通常有消磁器口品磁力不足的嚴重缺陷。
B. 消磁器口品可能未正確維護和操作。
C. 由於人為錯誤，無法在膛室中將驅動器轉向進行第二次掃描
D. 消毒媒體時記錄保存不足。
Answer: B (LEAVE A REPLY)
The most likely security issue with degaussing is that the degausser products may not be properly maintained and operated. Degaussing is a method of sanitizing magnetic media, such as hard disk drives, by applying a strong magnetic field that erases the data stored on the media.
Degaussing can be effective in destroying the data, but it requires that the degausser products are calibrated, tested, and used according to the manufacturer's specifications and instructions. If the

degausser products are not properly maintained and operated, they may not generate a sufficient magnetic force to erase the data completely, or they may damage the media or the device. Commercial products often have serious weaknesses of the magnetic force available in the degausser product, the inability to turn the drive around in the chamber for the second pass due to human error, and inadequate record keeping when sanitizing media are not the most likely security issues with degaussing, as they are related to the quality, the technique, or the documentation of the degaussing process, not the maintenance or the operation of the degausser products.

NEW QUESTION: 263
通訊網路中鏈路加密的優點是
A. 讓金鑰管理和分發更容易。
B. 從頭到尾保護整個網路的資料。
C. 提高傳輸效率。
D. 加密所有訊息，包括標頭和路由資訊。
Answer: D (LEAVE A REPLY)
An advantage of link encryption in a communications network is that it encrypts all information, including headers and routing information. Link encryption is a type of encryption that is applied at the data link layer of the OSI model, and encrypts the entire packet or frame as it travels from one node to another. Link encryption can protect the confidentiality and integrity of the data, as well as the identity and location of the nodes. Link encryption does not make key management and distribution easier, as it requires each node to have a separate key for each link. Link encryption does not protect data from start to finish through the entire network, as it only encrypts the data while it is in transit, and decrypts it at each node. Link encryption does not improve the efficiency of the transmission, as it adds overhead and latency to the communication.

NEW QUESTION: 264
使用自動化應用程式安全測試工具的主要優勢是什麼？
A. 應用程式可以在生口環境中受到保護。
B. 可以使用更少的資源來測試大量程式碼。
C. 使用這些工具進行測試時，應用程式的失敗率會降低。
D. 可以進行程式碼功能的詳細測試。
Answer: B (LEAVE A REPLY)
Automated application security testing tools are software tools that can scan, analyze, and test the code of an application for vulnerabilities, errors, or flaws. The primary advantage of using these tools is that they can test large amounts of code using fewer resources, such as time, money, and human effort, than manual testing. This can improve the efficiency, effectiveness, and coverage of the testing process. The application can be protected in the production environment, the application will fail less when tested using these tools, and detailed testing of code functions can be performed are all possible outcomes of using automated application security testing tools, but they are not the primary advantage of using them.

NEW QUESTION: 265
以下哪□最能描述系□安全□□中的“□□”概念？
A. □系□技□和非技□安全特性的正式、全面□估
B. 正式的管理决策，授□系□运行
C. 数据分□□□的分配□程
D. 媒体生命周期□束□□□媒体的□程
Answer: A (LEAVE A REPLY)
Certification is the comprehensive technical evaluation of a system's security controls to determine the extent to which they meet a set of specified requirements. Accreditation (or authorization) is the subsequent formal management decision to accept the risk and authorize the system to operate, based on the certification results.

NEW QUESTION: 266
下列哪一項描述了數位取證過程通常進行的順序？
A. 確定法律權限，商定審□策略，進行審□，報告結果
B. 確定法律權限，進行調□，報告結果，並同意審□策略
C. 商定審□策略、確定法律權限、進行審□並報告結果
D. 商定審□策略，確定法律權限，報告結果並進行審□
Answer: A (LEAVE A REPLY)
The digital forensic process is usually conducted in the following order: ascertain legal authority, agree upon examination strategy, conduct examination, and report results. This order ensures that the forensic process is lawful, ethical, and effective. The first step is to ascertain legal authority, which means to verify that the forensic examiner has the proper authorization, consent, or warrant to perform the examination. This step is crucial to avoid violating any laws or privacy rights of the data owner or custodian. The second step is to agree upon examination strategy, which means to define the scope, objectives, and methods of the examination. This step is important to establish the expectations, roles, and responsibilities of the forensic examiner and the client or stakeholder. The third step is to conduct examination, which means to collect, preserve, analyze, and document the digital evidence. This step is essential to perform the forensic tasks in a systematic, accurate, and reliable manner. The fourth step is to report results, which means to present the findings, conclusions, and recommendations of the examination. This step is necessary to communicate the forensic outcomes in a clear, concise, and understandable way.

NEW QUESTION: 267
下列哪一個程序中包含安全過程資料的收集是最重要的？
A. 季度訪問審核
B. 安全持續監控
C. 業務連續性測試
D. 年度安全培訓
Answer: (SHOW ANSWER)

Security continuous monitoring is the program in which it is most important to include the collection of security process data. Security process data is the data that reflects the performance, effectiveness, and compliance of the security processes, such as the security policies, standards, procedures, and guidelines. Security process data can include metrics, indicators, logs, reports, and assessments. Security process data can provide several benefits, such as:
Improving the security and risk management of the system by providing the visibility and awareness of the security posture, vulnerabilities, and threats Enhancing the security and decision making of the system by providing the evidence and information for the security analysis, evaluation, and reporting Increasing the security and improvement of the system by providing the feedback and input for the security response, remediation, and optimization Security continuous monitoring is the program in which it is most important to include the collection of security process data, because it is the program that involves maintaining the ongoing awareness of the security status, events, and activities of the system. Security continuous monitoring can enable the system to detect and respond to any security issues or incidents in a timely and effective manner, and to adjust and improve the security controls and processes accordingly. Security continuous monitoring can also help the system to comply with the security requirements and standards from the internal or external authorities or frameworks.

NEW QUESTION: 268
在網路漏洞評估的偵察階段，可以使用下列哪些命令列工具？
A. 挖掘
B. ifconfig
C. ipconfig
D. nbtstat
Answer: A (LEAVE A REPLY)
Dig is a command line tool that can be used in the reconnaissance phase of a network vulnerability assessment. Dig stands for domain information groper, and it is used to query Domain Name System (DNS) servers and obtain information about domains, hosts, and records.
Dig can help discover the network topology, the IP addresses, and the services running on the target network.

NEW QUESTION: 269
下列哪一種存取控制模型限制最多？
A. 自主存取控制 (DAC)
B. 強制存取控制 (MAC)
C. 基於角色的存取控制 (RBAC)
D. 基於規則的存取控制
Answer: B (LEAVE A REPLY)
Mandatory Access Control (MAC) is considered the most restrictive access control model because it enforces strict policies that are determined by the system or security administrator, rather than allowing users to make decisions about access.

In MAC, access to resources is governed by a centralized security policy. The system defines access controls based on classification levels (e.g., confidential, secret, top secret) and the user's clearance level, as well as specific labels on data. Users cannot change these permissions or grant access to others. This makes it more restrictive than the other models, as it leaves little room for user discretion. The restrictions imposed by MAC are rigid and typically enforced in high-security environments, such as military or government systems, where data classification and security are critical.

NEW QUESTION: 270
一個組織如果達到了能力成熟度模型整合(CMMI)4級，那麼它已經完成了下列哪些操作？
A. 針對持續創新流程改進
B. 解決了常見製程偏差的原因
C. 實現了最佳化的製程性能
D. 實現了可預測的流程效能
Answer: D (LEAVE A REPLY)
An organization that has achieved a Capability Maturity Model Integration (CMMI) level of 4 has done the following: achieved predictable process performance. CMMI is a framework that provides a set of best practices and guidelines for improving the capability and maturity of the processes of an organization, such as software development, service delivery, or project management. CMMI consists of five levels, each of which represents a different stage or degree of process improvement, from initial to optimized. The five levels of CMMI are:
Level 1: Initial. This level indicates that the processes of the organization are ad hoc, chaotic, or inconsistent, and that the outcomes of the processes are unpredictable, unreliable, or unrepeatable.
Level 2: Managed. This level indicates that the processes of the organization are planned, performed, measured, and controlled, and that the outcomes of the processes are manageable, stable, or repeatable.
Level 3: Defined. This level indicates that the processes of the organization are well-defined, documented, standardized, and integrated, and that the outcomes of the processes are aligned with the goals and objectives of the organization.
Level 4: Quantitatively Managed. This level indicates that the processes of the organization are quantitatively measured, analyzed, and optimized, and that the outcomes of the processes are predictable, consistent, or high-quality.
Level 5: Optimizing. This level indicates that the processes of the organization are continuously monitored, evaluated, and improved, and that the outcomes of the processes are innovative, adaptive, or excellent.
An organization that has achieved a CMMI level of 4 has done the following: achieved predictable process performance, meaning that the organization has established quantitative objectives and metrics for the processes, and has used statistical and analytical techniques to monitor and control the variation and performance of the processes, and to ensure that the processes meet the expected or desired outcomes. An organization that has achieved a CMMI level of 4 has not done the following: addressed continuous innovative process improvement, addressed the causes of common process

variance, or achieved optimized process performance, as these are the characteristics or achievements of a CMMI level of 5, which is the highest and most mature level of CMMI.

NEW QUESTION: 271
最大可容忍停機時間 (MTD) 決定什麼？
A. 在客□受到影響之前業務關鍵資料庫可以保持關閉的估計時間段。
B. 公司在沒有任何災難復原 (DR) 規劃的情況下可以承受災難的固定時間長度
C. 業務可能持續中斷的預計時段，超過該時段將面臨永遠無法復原的風險
D. □用冗餘系統之前災難復原過程中的固定時間長度
Answer: (SHOW ANSWER)
According to the CISSP For Dummies1, the Maximum Tolerable Downtime (MTD) determines the estimated period of time a business can remain interrupted beyond which it risks never recovering. This means that the MTD is the maximum acceptable duration of a disruption that the organization can tolerate before it suffers unacceptable consequences, such as loss of revenue, reputation, or customers. The MTD is an important input for the business continuity planning and disaster recovery planning processes, as it helps to define the recovery objectives and strategies for each business process and function. The MTD is not the same as the estimated period of time a business critical database can remain down before customers are affected, the fixed length of time a company can endure a disaster without any DR planning, or the fixed length of time in a DR process before redundant systems are engaged, as these are different concepts that may or may not be related to the MTD.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 272
以下哪□最能描述□用程序安全中的“□□□□漏洞”？
A. 完全由□□的加密□引起的漏洞
B. □用程序□期工作流程或□□中的缺陷可能被□用，□致出□非□期□果，即使□用程序完全按照代□运行，且不存在任何□□意□上的技□□□。
C. □影响底□数据□服□器的漏洞
D. 一种始□可被自□漏洞□描器□□到的漏洞□型
Answer: B (LEAVE A REPLY)
Business logic vulnerabilities are flaws in the intended workflow, rules, or assumptions underlying an application's functionality that can be exploited to achieve an unintended outcome-such as manipulating a shopping cart quantity to receive a negative price, or bypassing a required approval

step-even though the application code itself functions exactly as designed, making these vulnerabilities particularly difficult for automated scanners to detect, since they require understanding of the intended business context.

NEW QUESTION: 273
變革管理包含下列哪些口容？
A. 業務連續性測試
B. 實施前的使用者驗收測試 (UAT)
C. 企業主的技術審口
D. 實施後的成本效益分析 (CBA)
Answer: B (LEAVE A REPLY)
User Acceptance Testing (UAT) before implementation is one of the steps included in change management. Change management is a process that ensures that any changes to the system or the environment are planned, approved, tested, implemented, and documented in a controlled and consistent manner. UAT is a type of testing that involves the end users or the stakeholders of the system, and it verifies that the system meets the functional and non-functional requirements and expectations. UAT is usually performed before the implementation of the system or the change, as a final validation step.

NEW QUESTION: 274
雜湊訊息驗證碼 (HMAC) 使用下列哪種加密類型進行金鑰分發？
A. 對稱
B. 不對稱
C. 短暫的
D. 永久
Answer: A (LEAVE A REPLY)
Symmetric encryption is the type of encryption that is used in Hash Message Authentication Code (HMAC) for key distribution. Encryption is a technique that involves transforming the data or the message into an unreadable or unintelligible form, using a key and an algorithm, and that prevents unauthorized access, modification, or disclosure of the data or the message. Key distribution is a process that involves generating, exchanging, and managing the keys that are used for encryption and decryption, and that ensures that the keys are available and secure for the intended parties. HMAC is a technique that involves generating and appending a code or a tag to the data or the message, using a secret key and a hash function, and that verifies the integrity and the authenticity of the data or the message. Symmetric encryption is a type of encryption that uses the same key for both encryption and decryption, and that requires the key to be shared and agreed upon by both parties before the communication or the transaction.
Symmetric encryption is used in HMAC for key distribution, as it provides a fast and efficient way of encrypting and decrypting the data or the message, and of generating and verifying the code or the tag. Symmetric encryption can also reduce the complexity and the overhead of the key distribution process,

as it only requires one key to be exchanged and managed between the parties, instead of multiple keys.

NEW QUESTION: 275
在決定犯罪現場數位證據收集的優先順序時，法醫檢口員應先執行下列哪項活動？
A. 收集物證，
B. 建立波動順序。
C. 為現場人員分配職責。
D. 建立要檢口的檔案清單。
Answer: (SHOW ANSWER)
The order of volatility refers to the priority in which digital evidence should be collected based on how long it remains intact or how quickly it can be altered or destroyed. The key principle is that evidence that is most volatile (e.g., data in RAM, running processes, or live network connections) should be preserved first, as it may be lost or altered once the system is powered off or modified.

NEW QUESTION: 276
下列哪一項是資料管理員的職責？
A. 確保資料治理工作與組織保持一致。
B. 與組織進行資料治理訪談。
C. 記錄資料治理要求。
D. 確保將數據決策和影響力傳達給組織。
Answer: D (LEAVE A REPLY)
A data steward is responsible for managing and overseeing the organization's data assets, ensuring the data is accurate, accessible, secure, and used effectively. One of the key responsibilities of a data steward is to ensure that data decisions and impacts are communicated to the organization. This includes helping stakeholders understand the importance of data quality, the implications of data decisions, and how changes in data management affect the organization.
Data stewards serve as a bridge between data users, business units, and IT teams, ensuring that the organization's data-related policies, guidelines, and decisions are clearly communicated and understood.

NEW QUESTION: 277
下列哪一項事件促使對災難復原計畫 (DRP) 進行檢討？
A. 指導委員會新增成員
B. 安全性原則審核完成
C. 高階管理層變動
D. 組織合併
Answer: (SHOW ANSWER)
The event that prompts a review of the disaster recovery plan (DRP) is an organizational merger.

A DRP is a plan that defines the procedures and actions to be taken in the event of a disaster or a disruption, to restore the normal operations and services of an organization as quickly as possible. A DRP covers the aspects such as the roles and responsibilities, the recovery strategies and objectives, the backup and restoration methods, the communication and coordination channels, and the testing and maintenance schedules of the disaster recovery process. An organizational merger is an event that involves the combination or integration of two or more organizations into one single organization, as a result of a business decision or a strategy. An organizational merger prompts a review of the DRP, as it can affect the scope, scale, and complexity of the DRP, and require the alignment, consolidation, or modification of the DRP. A review of the DRP can help to ensure that the DRP is updated and consistent with the current and future needs and requirements of the merged organization, and that the DRP is effective and efficient for the disaster recovery process. New members added to the steering committee, completion of the security policy review, and change in senior management are not events that prompt a review of the DRP. These are some of the factors or changes that may influence or impact the DRP, but they are not as significant or critical as an organizational merger. New members added to the steering committee are individuals who join or replace the existing members of the steering committee, which is a group of people who oversee and guide the DRP and the disaster recovery process. Completion of the security policy review is a process that evaluates and revises the security policy, which is a document that defines the security goals, principles, and rules of an organization. Change in senior management is a situation that involves the replacement or reassignment of the senior management or the executives of an organization, who are responsible for the strategic and operational decisions and actions of the organization.

NEW QUESTION: 278
在檢口取證證據時，使用寫入阻止設備維護什麼？
A. 庫存
B. 完整性
C. 保密性
D. 可用性
Answer: B (LEAVE A REPLY)
Write blocking devices are used to prevent any modification of the forensic evidence when it is examined. This preserves the integrity of the evidence and ensures its admissibility in court. Write blocking devices do not affect the inventory, confidentiality, or availability of the evidence.

NEW QUESTION: 279
某組織正在外包其薪資系統，並要求對第三方資訊科技(IT) 系統進行全面審核。在盡職調口過程中，第三方提供了先前對其IT系統的審計報告。為了讓審核報告可接受，組織必須考慮下列哪一項？
A. 審計評估是由獨立評估員進行的。
B. 審計報告已由第三方高階管理層簽署。
C. 審計報告是在過去六個月口發布的。
D. 審計評估由國際審計公司進行。

Answer: A (LEAVE A REPLY)

The most important factor that the organization must consider in order for the audit reports to be acceptable is that the audit assessment has been conducted by an independent assessor. An independent assessor is a person or an entity that has no affiliation or interest with the third party or the organization, and that can perform the audit assessment objectively and impartially. An independent assessor can provide a credible and reliable evaluation of the third party's information technology (IT) systems, and identify any risks, issues, or gaps that may affect the security, performance, or compliance of the outsourced payroll system. An independent assessor can also verify that the third party's IT systems meet the organization's requirements and expectations, and that the third party follows the best practices and standards for IT security and management. The audit reports being signed by the third-party senior management, being issued in the last six months, or being conducted by an international audit firm are not as critical as the audit assessment being conducted by an independent assessor, as they do not guarantee the quality, validity, or relevance of the audit reports, or they may not be applicable or feasible in all cases.

NEW QUESTION: 280

下列哪一項是實施智慧卡時面臨的主要安全問題？

A. 這些卡片的記憶體有限。

B. 供應商應用程式相容性

C. 卡片可能會遺失

D. 移動代碼可以嵌入卡片中

Answer: C (LEAVE A REPLY)

The primary security concern associated with the implementation of smart cards is that the cards can be misplaced, lost, stolen, or damaged, resulting in the compromise of the user's identity, credentials, or data stored on the card.

NEW QUESTION: 281

災難復原 (DR) 流程應始終包括

A. 計畫維護。

B. 定期供應商審口。

C. 財務數據分析。

D. 定期庫存審核。

Answer: A (LEAVE A REPLY)

The disaster recovery (DR) process should always include plan maintenance. Plan maintenance is the process of updating, reviewing, testing, and improving the DR plan to ensure its effectiveness and efficiency. Plan maintenance is essential for the DR process, as it helps to keep the DR plan aligned with the current business needs, objectives, and environment, as well as the best practices and standards. Plan maintenance also helps to identify and resolve any gaps, issues, or weaknesses in the DR plan, as well as to incorporate any feedback, lessons learned, or changes from the previous DR tests or events. Plan maintenance should be performed regularly, as well as after any significant

changes in the organization, such as new systems, applications, processes, or personnel. Periodic vendor review, financial data analysis, and periodic inventory review are not activities that should always be included in the DR process.
Periodic vendor review is the process of evaluating the performance, quality, and reliability of the vendors that provide services or products to the organization, such as backup, recovery, or cloud services. Periodic vendor review is important for the DR process, as it helps to ensure that the vendors meet the contractual obligations and service level agreements (SLAs) of the organization, as well as to identify and mitigate any risks or issues associated with the vendors.
However, periodic vendor review is not a mandatory activity for the DR process, as it depends on the organization's reliance on external vendors for its DR strategy. Financial data analysis is the process of examining, interpreting, and reporting the financial data of the organization, such as revenue, expenses, assets, liabilities, or cash flow. Financial data analysis is important for the DR process, as it helps to determine the budget, resources, and priorities for the DR plan, as well as to measure the financial impact and return on investment (ROI) of the DR plan. However, financial data analysis is not a mandatory activity for the DR process, as it depends on the organization's financial goals and constraints for its DR strategy. Periodic inventory review is the process of verifying, updating, and documenting the inventory of the organization, such as hardware, software, data, or supplies. Periodic inventory review is important for the DR process, as it helps to ensure that the organization has the adequate and accurate inventory for its DR plan, as well as to identify and address any inventory shortages, surpluses, or discrepancies.
However, periodic inventory review is not a mandatory activity for the DR process, as it depends on the organization's inventory management and control for its DR strategy.

NEW QUESTION: 282
如果員工因違反組織的可接受使用政策 (ALP) 而被解僱，下列哪一項至關重要？
A. 權限暫停
B. 網際網路存取日誌
C. 代理程式記錄
D. 適當的文檔
Answer: D (LEAVE A REPLY)
Appropriate documentation is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (AUP). An AUP is a policy that defines the acceptable and unacceptable use of the organization's information systems and resources by the employees. A violation of the AUP can result in disciplinary actions, such as warnings, suspension, or termination. Appropriate documentation can provide evidence of the violation, the investigation process, the communication with the employee, and the decision of the dismissal. Appropriate documentation can also protect the organization from legal challenges or disputes from the dismissed employee.

NEW QUESTION: 283
以下哪□最能描述“接受授予”□□控制模型？
A. 一种□□关注网□分割的模型

B. 一种使用有向□来表示□利如何□移(“取得”)或“□得”的正式模型
主体和客体之□的“授予”
C. 一种完全消除所有□概念的模式
D. □用于物理安全的模型
Answer: B (LEAVE A REPLY)
The Take-Grant model is a formal access control model that represents subjects, objects, and their access rights as a directed graph, defining specific rules (take, grant, create, remove) that govern how rights can be transferred between subjects and objects, allowing analysts to formally determine whether a given right could ever be propagated to an unauthorized subject.

NEW QUESTION: 284
一家組織最近升級到了網際網路協定語音 (VoIP) 電話系統。
管理層關注未經授權的電話使用。安全顧問負責制定保護這些手機的計畫。管理員為組織中的每個人分配了唯一的個人識別號碼。最好的解決方案是什麼？
A. 使用手機鎖定軟體強制執行使用和 PIN 策略。
B. 通知使用者定期更改PIN。實施呼叫詳細記錄 (CDR) 報告以追蹤使用情況。
C. 請管理者強制執行定期變更 PIN 的策略。實施呼叫詳細記錄 (CDR) 報告以追蹤使用情況。
D. 請管理員定期更改 PIN。實施呼叫詳細記錄 (CDR) 報告以追蹤使用情況。
Answer: A (LEAVE A REPLY)
The best solution to secure the VoIP phones and prevent unauthorized phone usage is to use phone locking software to enforce usage and PIN policies. Phone locking software can restrict the access to the phone features and functions based on the user's PIN, role, or location. Phone locking software can also enforce policies such as PIN expiration, PIN complexity, PIN history, and PIN lockout. Phone locking software can also generate logs and reports of the phone usage and activity. This way, the phone locking software can enhance the security, accountability, and compliance of the VoIP phone system . The other solutions are not as effective, because they rely on the user or the administrator to change the PIN regularly, which may not be feasible, consistent, or secure. Implementing call detail records (CDR) reports to track usage is a good practice, but it does not prevent unauthorized phone usage in the first place.

NEW QUESTION: 285
實施變革管理的主要原因是什麼？
A. 驗證並批准向環境的發布
B. 提供系統變更版本回滾
C. 確保所有申請獲得批准
D. 確保對環境變化負責
Answer: D (LEAVE A REPLY)
Ensuring accountability for changes to the environment is the primary reason for implementing change management. Change management is a process that ensures that any changes to the system or

network environment, such as the hardware, software, configuration, or documentation, are planned, approved, implemented, and documented in a controlled and consistent manner.
Change management can provide several benefits, such as:
Improving the security and reliability of the system or network environment by preventing or reducing the errors, conflicts, or disruptions that might occur due to the changes Enhancing the performance and efficiency of the system or network environment by optimizing the resources and functions Increasing the compliance and alignment of the system or network environment with the internal or external requirements and standards Facilitating the monitoring and improvement of the system or network environment by tracking and logging the changes and their outcomes Ensuring accountability for changes to the environment is the primary reason for implementing change management, because it can ensure that the changes are authorized, justified, and traceable, and that the parties involved in the changes are responsible and accountable for their actions and results. Accountability can also help to deter or detect any unauthorized or malicious changes that might compromise the system or network environment.

NEW QUESTION: 286
關於點對點微波傳輸，下列哪一個敘述是正確的？
A. 由於加密，它們不會被攔截
B. 攔截僅取決於訊號強度。
C. 它們的重複使用程度太高，無法進行有效的攔截
D. 它們容易被附近的天線攔截。
Answer: D (LEAVE A REPLY)
They are subject to interception by an antenna within proximity. Point-to-point microwave transmissions are line-of-sight media, which means that they can be intercepted by any antenna that is in the direct path of the signal. The interception does not depend on encryption, multiplexing, or signal strength, as long as the antenna is close enough to receive the signal.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 287
在專案風險評估階段，首席資訊安全長(CISO) 發現大學口某學院正在透過其口部開發的應用程式收集受保護的健康資訊 (PHI) 資料。該學院完全了解 《健康保險流通與責任法案》(HIPAA) 的相關規定，並完全遵守該法案。CISO 的最佳應對方案是什麼？
A. 將此系統記錄為高風險

B. 執行漏洞評估
C. 進行定量威脅評估
D. 記錄資訊並繼續
Answer: D (LEAVE A REPLY)
The best approach for the CISO is to notate the information and move on. A CISO is a Chief Information Security Officer, who is a senior executive responsible for overseeing and managing the information security strategy, policies, and programs of an organization. A risk assessment is a process of identifying, analyzing, and evaluating the risks that may affect the information and assets of an organization. In this scenario, the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant. HIPAA is a federal law that sets the standards and rules for the protection and privacy of PHI, which is any information that can be used to identify a person's health condition, treatment, or payment. The best approach for the CISO is to notate the information and move on, as there is no need to take any further action or intervention, since the college is already compliant with the HIPAA regulations and has implemented the appropriate security measures for the PHI data.

NEW QUESTION: 288
下列哪一項是安全控制波動性？
A. 安全控制穩定性的參考。
B. 表示安全控制的不可預測性。
C. 安全控制影響的引用。
D. 安全控制發生變化的可能性的參考。
Answer: (SHOW ANSWER)
Security control volatility is a reference to the likelihood of change in the security control. Security control volatility is a factor that affects the selection, implementation, and maintenance of security controls in an organization. Security control volatility can be influenced by various internal and external factors, such as business needs, technology trends, regulatory requirements, threat landscape, and risk appetite. Security control volatility can have implications for the security posture, performance, and cost of the organization.

NEW QUESTION: 289
以下四個迭代步驟中哪一個是對第三方供應商持續進行的？
A. 調口、評估、回應、監控
B. 框架、評估、回應、監控
C. 框架、評估、修復、監控
D. 調口、評估、修復、監控
Answer: B (LEAVE A REPLY)

Third-party vendors are external entities that provide products or services to an organization, such as suppliers, contractors, consultants, or partners. Third-party vendors can pose various risks to the organization, such as security breaches, compliance violations, service disruptions, or reputational damage. Therefore, the organization should conduct a third-party risk management (TPRM) process to identify, assess, mitigate, and monitor the risks associated with third-party vendors. The TPRM process consists of four iterative steps that are conducted on third-party vendors in an on-going basis. The steps are:
Frame: This step involves defining the scope, objectives, and governance of the TPRM process, as well as establishing the criteria and thresholds for risk assessment and acceptance.
Assess: This step involves collecting and analyzing information about the third-party vendors, such as their security policies, controls, practices, certifications, and performance, to evaluate their risk profile and compliance status.
Respond: This step involves developing and implementing strategies and actions to address the risks identified in the assessment step, such as negotiating contracts, enforcing service level agreements, applying controls, conducting audits, or terminating relationships.
Monitor: This step involves tracking and reviewing the performance and risk posture of the third- party vendors on a regular basis, as well as updating the TPRM process as needed to reflect changes in the business environment, regulatory requirements, or risk appetite.
Therefore, the correct answer is B.

NEW QUESTION: 290
最近離開該組織的一位同事向安全專業人員索取一份該組織的機密事件管理策略的副本。下列哪一項是對此請求的最佳回應？
A. 透過電子郵件將政策發送給同事，因為他們已經是組織的一部分並且熟悉該政策。
B. 不確認收到前同事的請求並忽略它們。
C. 在公司發放的設備上存取政策並讓前同事口看螢幕。
D. 透過公司官方管道提交請求，以確保政策可以分發。
Answer: D (LEAVE A REPLY)
The best response to the request from a former colleague for a copy of the organization's confidential incident management policy is to submit the request using company official channels to ensure the policy is okay to distribute. The incident management policy is a policy that defines the roles, responsibilities, and procedures for the identification, response, and recovery of the security incidents that may affect the organization. The incident management policy is a confidential document that contains sensitive information and data, and that should be protected from unauthorized access, disclosure, or modification. Submitting the request using company official channels can help to ensure the policy is okay to distribute, as it can verify the legitimacy and validity of the request, and the authorization and clearance of the requester. Submitting the request using company official channels can also help to comply with the security policies and standards, and the legal, regulatory, or contractual requirements of the organization, and to prevent or mitigate any potential security risks or issues that may arise from the distribution of the policy.

NEW QUESTION: 291
組織進行安全審計的主要目的是什麼？
A. 確保組織遵守明確的標準
B. 確保組織正在應用安全控制來減輕已識別的風險
C. 確保組織有效配置資訊系統
D. 確保組織記錄調口結果
Answer: B (LEAVE A REPLY)
The primary purpose for an organization to conduct a security audit is to ensure that the organization is applying security controls to mitigate identified risks. A security audit is a systematic and independent examination of the security posture and performance of an organization, system, or network, against a set of predefined criteria, standards, or regulations. A security audit can help to ensure that the organization is applying security controls to mitigate identified risks, by evaluating the effectiveness and adequacy of the security controls and measures that are implemented on the organization, system, or network, and by identifying and resolving any security issues or gaps that may expose the organization, system, or network to various security threats and risks. A security audit can also help to provide recommendations and solutions to improve the security posture and performance of the organization, system, or network, as well as to demonstrate the compliance and accountability of the organization with the relevant security policies and regulations. To ensure the organization is adhering to a well-defined standard, to ensure the organization is configuring information systems efficiently, or to ensure the organization is documenting findings are not the primary purposes for an organization to conduct a security audit, as they are more related to the quality, optimization, or reporting aspects of security.

NEW QUESTION: 292
安全分發對稱加密金鑰需要下列哪一項？
A. 官方批准的公鑰基礎設施 (PKI) 3 類或 4 類證書
B. 官方批准且合規的金鑰管理技術和流程
C. 組織核准的通訊保護策略與金鑰管理計劃
D. 保護使用者私鑰的硬體令牌。
Answer: B (LEAVE A REPLY)
According to the CISSP All-in-One Exam Guide, the thing that is needed to securely distribute symmetric cryptographic keys is officially approved and compliant key management technology and processes. Symmetric cryptography is a type of cryptography that uses the same key to encrypt and decrypt the data or information, such as the Advanced Encryption Standard (AES) or the Data Encryption Standard (DES). Symmetric cryptographic keys are the secret or random values that are used to perform the encryption and decryption operations, such as the 128-bit or 256-bit keys. Key management is the process of generating, distributing, storing, using, changing, and destroying the cryptographic keys, as well as the policies and procedures that govern the process. Key management technology and processes are the tools and methods that are used to implement and perform the key management process, such as the key distribution protocols, the key servers, or the key lifecycle models. Key management technology and processes need to be officially approved and compliant, which means that they need to meet the standards, regulations, and requirements that are

established by the authorities or organizations that oversee or regulate the cryptography or the security of the data or information, such as the National Institute of Standards and Technology (NIST) or the Payment Card Industry Data Security Standard (PCI DSS). Officially approved and compliant key management technology and processes are needed to securely distribute symmetric cryptographic keys, as they ensure that the keys are generated, distributed, stored, used, changed, and destroyed in a secure and consistent manner, and that the keys are protected from unauthorized or unintended access, disclosure, modification, corruption, loss, or theft. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates are not the things that are needed to securely distribute symmetric cryptographic keys, although they may be the things that are needed to securely distribute asymmetric cryptographic keys. PKI is a system or a framework that provides the services and mechanisms for the creation, management, distribution, and verification of the digital certificates, which are the electronic documents that bind the identity and the public key of an entity, such as a person, a device, or an organization. PKI uses asymmetric cryptography, which is a type of cryptography that uses a pair of keys to encrypt and decrypt the data or information, such as the Rivest- Shamir-Adleman (RSA) or the Elliptic Curve Cryptography (ECC). Asymmetric cryptographic keys are the public or private values that are used to perform the encryption and decryption operations, such as the 2048-bit or 4096-bit keys. PKI certificates are classified into different classes or levels, based on the identity verification and assurance requirements, such as Class 1, Class 2, Class 3, or Class 4. Class 3 and Class 4 certificates are the highest classes or levels of PKI certificates, which require the most rigorous and stringent identity verification and assurance processes, such as the face-to-face or the in-person verification. Class 3 and Class 4 certificates are used for the high- security or high-value applications or transactions, such as the e- commerce, the e-government, or the e-banking. Class 3 and Class 4 certificates may help to securely distribute asymmetric cryptographic keys, as they ensure that the public keys are authentic, valid, and trustworthy, and that the identity and the public key of the entity are properly and securely bound. However, Class 3 and Class 4 certificates are not the things that are needed to securely distribute symmetric cryptographic keys, as they are not related to the symmetric cryptography or the symmetric cryptographic keys. An organizationally approved communication protection policy and key management plan is not the thing that is needed to securely distribute symmetric cryptographic keys, although it may be a document that guides or supports the key management technology and processes. A communication protection policy is a document that defines the rules, principles, and guidelines for the protection of the data or information that is transmitted or received over the communication channels or networks, such as the encryption, authentication, or integrity methods or mechanisms. A key management plan is a document that defines the objectives, scope, roles, and responsibilities for the key management process, as well as the policies and procedures for the key management process, such as the key generation, distribution, storage, use, change, and destruction policies and procedures. An organizationally approved communication protection policy and key management plan may help to guide or support the key management technology and processes, but it is not the thing that is needed to securely distribute symmetric cryptographic keys, as it is not the tool or method that is used to implement or perform the key management process. Hardware tokens that protect the user's private key are not the things that are needed to securely distribute symmetric cryptographic keys, although they may be the things that are

used to store or use the symmetric cryptographic keys. Hardware tokens are the physical or tangible devices that are used to store or use the cryptographic keys, such as the smart cards, the USB drives, or the hardware security modules.
Hardware tokens may help to protect the user's private key, which is the asymmetric cryptographic key that is used to decrypt the data or information, or to sign the data or information, such as the RSA or the ECC private key. Hardware tokens may also help to store or use the symmetric cryptographic key, which is the symmetric cryptographic key that is used to encrypt and decrypt the data or information, such as the AES or the DES key. However, hardware tokens are not the things that are needed to securely distribute symmetric cryptographic keys, as they are not the tools or methods that are used to generate or distribute the symmetric cryptographic keys.

NEW QUESTION: 293
下列何者能□為無線區域網路 (WLAN) 提供有效的管理保障？
A. 維護已授權存取點 (AP) 和連接裝置的清單
B. 將無線電頻率設定為所需的最小範圍
C. 在 WLAN 用□端裝置和 VPN 集中器之間建立虛擬私人網路 (VPN) 隧道
D. 正在驗證所有預設密碼是否已更改
Answer: C (LEAVE A REPLY)
The action that provides effective management assurance for a WLAN is establishing a VPN tunnel between the WLAN client device and a VPN concentrator. A VPN is a secure and encrypted connection that enables remote access to a private network over a public network, such as the internet. A VPN concentrator is a device that manages and authenticates the VPN connections, and provides encryption and decryption services. By establishing a VPN tunnel, the organization can protect the confidentiality, integrity, and availability of the data transmitted over the WLAN, and prevent unauthorized or malicious access to the network.

NEW QUESTION: 294
在系統管理審計過程中，審計人員發現系統管理員未接受過相關訓練 為確保系統完整性，需要立即採取哪些措施？
A. 對招募政策和新員工核實方法的審□
B. 對所有部門程序的審□
C. 對所有待進行的訓練程序進行審□
D. 由經驗豐富的管理員對所有系統進行審□
Answer: (SHOW ANSWER)
During an audit of system management, if auditors find that the system administrator has not been trained, the immediate action that needs to be taken to ensure the integrity of systems is a review of all systems by an experienced administrator. This is to verify that the systems are configured, maintained, and secured properly, and that there are no errors, vulnerabilities, or breaches that could compromise the system's availability, confidentiality, or integrity. A review of hiring policies, departmental procedures, or training procedures are not urgent actions, as they are more related to the long-term improvement of the system management process, rather than the current state of the systems.

NEW QUESTION: 295
經過數位簽署的電子郵件透過有線等效保密 (WEP) 協定保護的無線網路傳送。下列哪一項原則有風險？
A. 可用性
B. 不可否認性
C. 保密性
D. 完整性
Answer: C (LEAVE A REPLY)
Confidentiality is the principle that is at risk when a digitally-signed e-mail is delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Confidentiality is the principle that ensures that the data or information is only accessible or disclosed to authorized parties, and that it is protected from unauthorized access or disclosure. WEP is an outdated and insecure protocol that encrypts the wireless network traffic using a shared key that can be easily cracked or compromised by attackers. If an attacker intercepts the wireless network traffic, they can decrypt the WEP-encrypted packets and read the contents of the e-mail, which may contain sensitive or confidential information.

NEW QUESTION: 296
以下哪一項最適當地描述了為什麼軟體保障對於幫助防止組織業務和任務風險的增加至關重要？
A. 未如預期運作的軟體可能會被利用，從而容易受到攻擊。
B. 徵求建議書 (RFP) 避免購買無法滿足業務需求的軟體。
C. 簽約流程消除了購買者對安全漏洞的責任。
D. 舊軟體的退役可以降低與技術債相關的長期成本。
Answer: (SHOW ANSWER)
Software assurance is the process of ensuring that software is designed, developed, and maintained in a secure manner that minimizes the risk of vulnerabilities and defects. Software assurance helps prevent an increase in business and mission risk for an organization by reducing the likelihood and impact of successful attacks that could compromise the confidentiality, integrity, or availability of the software and the data it processes. Software assurance also helps ensure that the software meets the functional and nonfunctional requirements of the organization and its stakeholders.

NEW QUESTION: 297
在評估應用程式的審核能力時，下列哪項活動最重要？
A. 確定審核記錄是否包含足□的資訊。
B. □看安全性計劃，以了解審核失敗時要採取的操作。
C. 驗證是否為審核記錄分配了足□的儲存空間。
D. 確定調□可疑活動的程序。
Answer: A (LEAVE A REPLY)
Audit capability is the ability of a system or application to generate and store audit records that can be used to monitor, analyze, and investigate the activities and events that occur within the system or application. Audit records should contain sufficient information to identify the who, what, when, where,

and how of each auditable event. This information is essential for accountability, nonrepudiation, and forensic analysis. Therefore, when assessing the audit capability of an application, the most important activity is to determine if the audit records contain sufficient information. Reviewing the security plan for actions to be taken in the event of audit failure, verifying if sufficient storage is allocated for audit records, and identifying procedures to investigate suspicious activity are also important activities, but they are secondary to the quality of the audit records.

NEW QUESTION: 298
網際網路通訊協定 (IP) 來源位址欺騙被用於繞過安全防護。
A. 基於地址的身份驗證。
B. 位址解析協定(ARP)。
C. 反向位址解析協定(RARP)。
D. 傳輸控制協定(TCP)劫持。
Answer: A (LEAVE A REPLY)
Internet Protocol (IP) source address spoofing is used to defeat address-based authentication, which is a method of verifying the identity of a user or a system based on their IP address. IP source address spoofing involves forging the IP header of a packet to make it appear as if it came from a trusted or authorized source, and bypassing the authentication check. IP source address spoofing can be used for various malicious purposes, such as denial-of-service attacks, man-in- the-middle attacks, or session hijacking.

NEW QUESTION: 299
哪種類型的風險與組織中進行的增口和管理活動的順序有關？
A. 需求風險
B. 流程風險
C. 控制風險
D. 供應風險
Answer: B (LEAVE A REPLY)
The type of risk that is related to the sequences of value-adding and managerial activities undertaken in an organization is process risk. Process risk is the risk that arises from the inefficiency, inadequacy, or failure of the processes that are performed by the organization to achieve its objectives and deliver its products or services. Process risk can affect the quality, performance, and security of the organization's outputs and outcomes, and can result in financial, operational, or reputational losses or damages. Process risk can be caused by various factors, such as human errors, system errors, design flaws, compliance issues, or external events.
Process risk can be managed by implementing and monitoring the process controls, such as policies, procedures, standards, or metrics, that ensure the effectiveness, efficiency, and reliability of the processes.

NEW QUESTION: 300

下列哪一項是網路上執行的嗅探器僅從自己的主機收集資料包的主要原因？
A. 入侵偵測系統 (IDS) 已丟棄資料包。
B. 使用交換器連接網路。
C. 網路使用集線器連接。
D. 網路防火牆不允許嗅探。
Answer: A (LEAVE A REPLY)
The primary reason a sniffer operating on a network is collecting packets only from its own host is that the network is connected using switches. A sniffer is a tool that captures and analyzes the network traffic by intercepting the packets that flow through the network. A sniffer can be used for various purposes, such as network troubleshooting, performance monitoring, security auditing, or malicious activities. The network topology and the devices used to connect the network affect the ability and the scope of the sniffer to capture the packets. A switch is a device that connects multiple devices on a network and forwards the packets to the destination device based on the MAC address. A switch creates separate collision domains for each port, which means that the packets are only sent to the intended device and not to the others. Therefore, a sniffer connected to a switch can only capture the packets that are destined for or originated from its own host, unless the switch is configured to allow port mirroring or broadcast the packets to all ports.

NEW QUESTION: 301
安全團隊計劃在企業用口存取審核流程中使用自動帳口對帳。為了在執行審核時獲得最佳結果和最少錯誤，必須實施下列哪一項？
A. 從審核中刪除服務帳口
B. 職責分離 (SoD)
C. 明確的設定策略
D. 頻繁審核
Answer: C (LEAVE A REPLY)
Clear provisioning policies are essential for the best results with fewest errors when running the audit using automated account reconciliation. Automated account reconciliation is a process that compares the user accounts and access rights in the system with the expected or authorized accounts and access rights, and identifies any discrepancies or anomalies. Clear provisioning policies define the rules and criteria for creating, modifying, deleting, and reviewing user accounts and access rights, and they provide a baseline for the automated account reconciliation process.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 302
在軟體口品的開發階段，下列哪一項用於支援縱深防禦的概念？
A. 維護掛鉤
B. 多機構化
C. 已知漏洞列表
D. 安全審核
Answer: (SHOW ANSWER)
Defense in depth is a security strategy that employs multiple layers of security controls and mechanisms to protect the system or network from various types of attacks. Defense in depth can be applied during the development phase of a software product by using security auditing as a technique to support the concept. Security auditing is a process of reviewing and evaluating the security aspects of the software product, such as the design, code, functionality, performance, or compliance. Security auditing can help to identify and fix any security vulnerabilities or flaws in the software product, as well as to ensure that the software product meets the security requirements and standards of the organization and the stakeholders. Security auditing can be performed by internal or external auditors, using manual or automated tools, methods, or frameworks. Maintenance hooks, polyinstantiation, or known vulnerability list are not used to support the concept of defense in depth during the development phase of a software product, as they are more related to maintenance, data security, or vulnerability management.

NEW QUESTION: 303
身分和存取配置生命週期的第二步是什麼？
A. 配置
B. 回顧
C. 核准
D. 撤銷
Answer: C (LEAVE A REPLY)
The identity and access provisioning lifecycle is the process of managing the creation, modification, and termination of user accounts and access rights in an organization. The second step in this lifecycle is approval, which means that the identity and access requests must be authorized by the appropriate managers or administrators before they are implemented. Approval ensures that the principle of least privilege is followed and that only authorized users have access to the required resources.

NEW QUESTION: 304
下列哪一項決定了流量應如何依照基礎設施的狀態流動？
A. 應用平面
B. 資料平面
C. 控制平面
D. 交通平面
Answer: C (LEAVE A REPLY)

The control plane is the part of a network that determines how traffic should flow based on the status of the infrastructure. The control plane consists of the protocols, algorithms, and policies that are used to calculate the best paths, routes, and forwarding decisions for the network traffic.
The control plane communicates with the data plane, which is the part of the network that actually carries the traffic from the source to the destination. The control plane also communicates with the management plane, which is the part of the network that monitors, configures, and maintains the network devices and components. The control plane is the best answer among the given options to the question of which part of the network determines how traffic should flow based on the status of the infrastructure. The application plane is not a part of the network, but rather a layer of the Open Systems Interconnection (OSI) model that provides the interface and functionality for the network applications and services. The application plane does not determine how traffic should flow, but rather what type of traffic is generated or consumed by the applications and services. The data plane is the part of the network that actually carries the traffic from the source to the destination, as mentioned above. The data plane does not determine how traffic should flow, but rather executes the forwarding decisions made by the control plane. The traffic plane is not a part of the network, but rather a term that refers to the overall flow of traffic in the network. The traffic plane does not determine how traffic should flow, but rather reflects the result of the control plane and the data plane operations.

NEW QUESTION: 305
下列哪一項是區域網路 (LAN) 中透過分段提供額外安全等級的常見措施？
A. 建置虛擬區域網路 (VLAN)
B. 建立非軍事區 (DMZ)
C. 實施病毒掃描程序
D. 實施入侵偵測系統 (IDS)
Answer: (SHOW ANSWER)
Building Virtual Local Area Networks (VLAN) is a common measure within a Local Area Network (LAN) to provide an additional level of security through segmentation. A VLAN is a logical grouping of network devices that share the same broadcast domain, regardless of their physical location or connection. A VLAN can be used to segment a LAN into smaller subnetworks based on criteria such as function, department, or security level. A VLAN can enhance the security of a LAN by isolating the traffic and data of different groups, preventing unauthorized access or communication, reducing the attack surface, and improving the performance and manageability of the network.

NEW QUESTION: 306
Web 應用程式要求使用者在使用其服務之前進行註冊。使用者必須選擇唯一的使用者名稱和至少包含八個字元的密碼。必須使用哪種方法來儲存這些密碼以確保離線攻擊變得困難？
A. 使用快速的加密演算法以及隨機的每個使用者加密金鑰。
B. 使用快速的雜湊函數以及每個使用者的隨機鹽。
C. 使用具有成本因子和每個用口隨機鹽的雜湊函數。
D. 使用隨機主金鑰的加密演算法。

Answer: C (LEAVE A REPLY)
Active discovery is identifying and cataloging assets within an organization's environment. This can be done manually or through the use of automated tools. The goal of active discovery is to create an accurate inventory of all devices and software within the network.

NEW QUESTION: 307
下列哪一項實踐提供了軟體設計中的安全開發和威脅識別？
A. 利害關係人審核
B. 要求審核
C. 滲透測試
D. 威脅建模
Answer: D (LEAVE A REPLY)
Threat modeling is a practice that provides the development of security and identification of threats in designing software. Threat modeling is a systematic process of identifying, analyzing, and mitigating the potential threats and vulnerabilities that could affect a software system. Threat modeling helps to design secure software by applying security principles, such as defense in depth, least privilege, and fail-safe defaults, throughout the software development life cycle.
Stakeholder review, requirements review, and penetration testing are not practices that provide the development of security and identification of threats in designing software, although they may contribute to the overall security assurance of the software. Stakeholder review is a process of obtaining feedback and approval from the stakeholders of a software project, such as customers, users, managers, and developers. Requirements review is a process of verifying and validating the functional and non- functional requirements of a software system, such as performance, usability, reliability, and security. Penetration testing is a process of simulating real-world attacks on a software system to identify and exploit its vulnerabilities and weaknesses.

NEW QUESTION: 308
下列哪一項被視為治理、風險管理和合規 (GRC) 計畫的最後一道防線？
A. □部稽核
B. □部控制
C. 董事會審□
D. 風險管理
Answer: A (LEAVE A REPLY)
Internal audit is considered the last line of defense in regard to a governance, risk management, and compliance (GRC) program. Internal audit is an independent and objective function that provides assurance and consulting services to the organization. Internal audit evaluates the effectiveness and efficiency of the GRC program, identifies gaps and weaknesses, and recommends improvements. Internal audit also reports to the senior management and the board of directors on the status and results of the GRC program.

NEW QUESTION: 309

一位安全專業人員正在評估應用程式中的風險，但未考慮任何緩解或補償控制措施。此類風險評級屬於下列哪一項的範例？

A. 轉移風險

B. 固有風險

C. 殘留風險

D. 避免風險

Answer: B (LEAVE A REPLY)

Inherent risk is the risk that exists in an application or a system before applying any mitigating or compensating controls. Inherent risk represents the worst-case scenario of the potential impact and likelihood of a threat exploiting a vulnerability. Inherent risk is usually assessed by using qualitative or quantitative methods, such as risk matrices, risk scales, or risk formulas. Inherent risk helps to identify the areas that need the most attention and resources, and to prioritize the implementation of controls. Inherent risk is different from residual risk, which is the risk that remains after applying the controls, and from transferred risk, which is the risk that is shifted to another party, such as an insurance company or a service provider. Inherent risk is also different from avoided risk, which is the risk that is eliminated by not performing an activity or by changing the scope or objectives of the activity.

NEW QUESTION: 310

當道德駭客不了解目標系統但在測試前通知測試目標時，正在執行哪種類型的安全測試？

A. 反轉

B. 灰框

C. 盲

D. 白盒

Answer: C (LEAVE A REPLY)

The scenario described seems to match the concept of "Blind" testing, except for the fact that the target is notified beforehand. Typically, in Blind testing, the ethical hacker has no prior knowledge of the system, and the target is unaware of when the test will occur.

However, if we strictly follow the given details that the target is notified before the test and the ethical hacker has no knowledge, this seems to align more closely with a Blind test, but with prior notification being a slight variant on the usual practice.

NEW QUESTION: 311

如果員工從一個角色轉移到另一個角色，這應該在身分和存取管理(IAM) 生命週期□觸發下列哪些操作？

A. 新帳□創建

B. 使用者存取權限審核與調整

C. 取消配置

D. 系統帳號存取權限審核與調整

Answer: B (LEAVE A REPLY)

User access review and adjustment is the action that should be triggered within the identity and access management (IAM) lifecycle when an employee transfers from one role to another. IAM is the process

of identifying, authenticating, authorizing, and managing the users and their access rights to the organization's resources and systems. The IAM lifecycle consists of four phases: provisioning, maintenance, review, and deprovisioning. When an employee transfers from one role to another, their access rights may need to be changed or updated to reflect their new responsibilities and duties. This requires a user access review and adjustment, which is part of the maintenance phase of the IAM lifecycle. User access review and adjustment involves verifying and validating the user's identity and current access rights, and modifying or revoking the access rights as needed, based on the principle of least privilege and the organization's policies and standards.

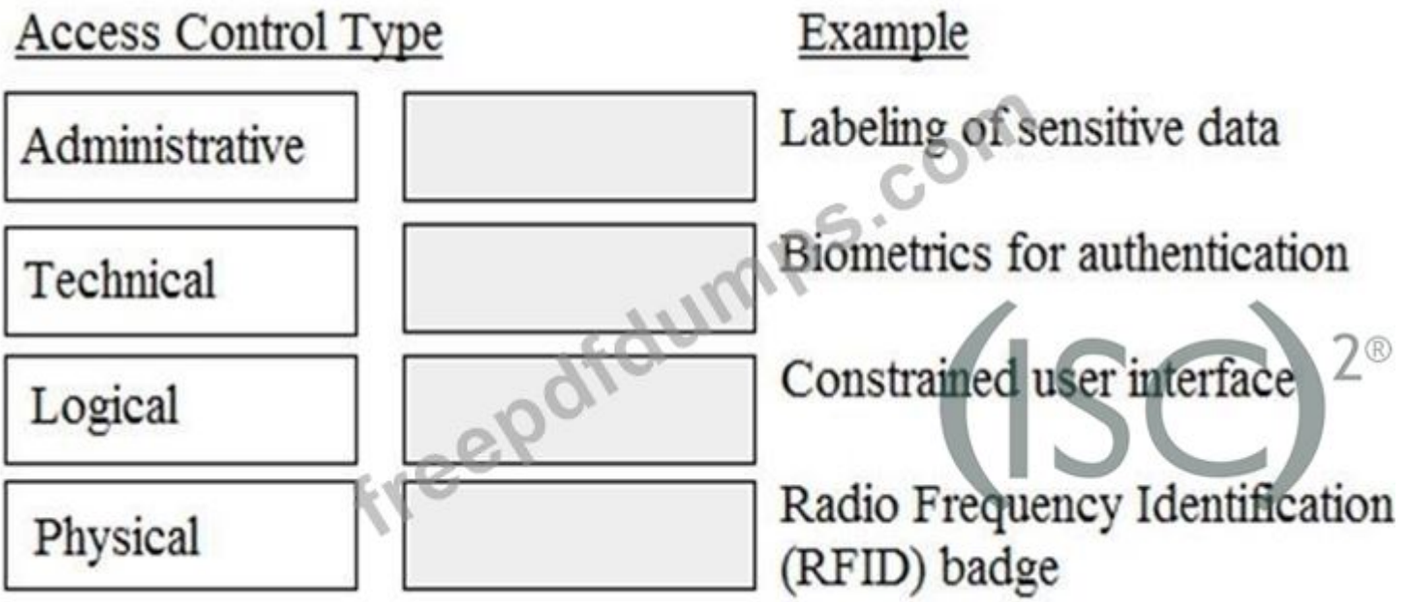
NEW QUESTION: 312
某個組織發現，組織資料由員工發佈到公眾可存取的資料儲存。組織必須採取哪些主要步驟來確保資料得到適當保護，不被公開發布？
A. 實施資料分類策略。
B. 實施資料加密策略。
C. 實施使用者訓練政策。
D. 實施使用者報告政策。
Answer: A (LEAVE A REPLY)
A data classification policy is the primary step an organization must take to ensure data is properly protected from public release, because it defines the levels of sensitivity and confidentiality of the data, and the corresponding security controls and handling requirements. A data encryption policy, a user training policy, and a user reporting policy are all important measures to protect data, but they are secondary to the data classification policy, which sets the foundation for data protection.

NEW QUESTION: 313
視網膜掃描生物辨識設備測量的是哪一種生理特徵？
A. 視網膜反射的光量
B. 視網膜的大小、曲率和形狀
C. 眼後部血管的分佈模式
D. 眼睛後部感光細胞的分佈模式
Answer: C (LEAVE A REPLY)
A retinal scan is a biometric technique that uses unique patterns on a person's retina blood vessels to identify them. The retina is a thin layer of tissue at the back of the eye that contains millions of light-sensitive cells and blood vessels. The retina converts the light rays that enter the eye into electrical signals that are sent to the brain for visual processing78 The pattern of blood vessels in the retina is not genetically determined and varies from person to person, even among identical twins. The retina also remains unchanged from birth until death, unless affected by some diseases or injuries. Therefore, the retina is considered to be one of the most accurate and reliable biometrics, apart from DNA78 A retinal scan is performed by projecting a low-energy infrared beam of light into a person's eye as they look through the scanner's eyepiece. The beam traces a standardized path on the retina, and the amount of

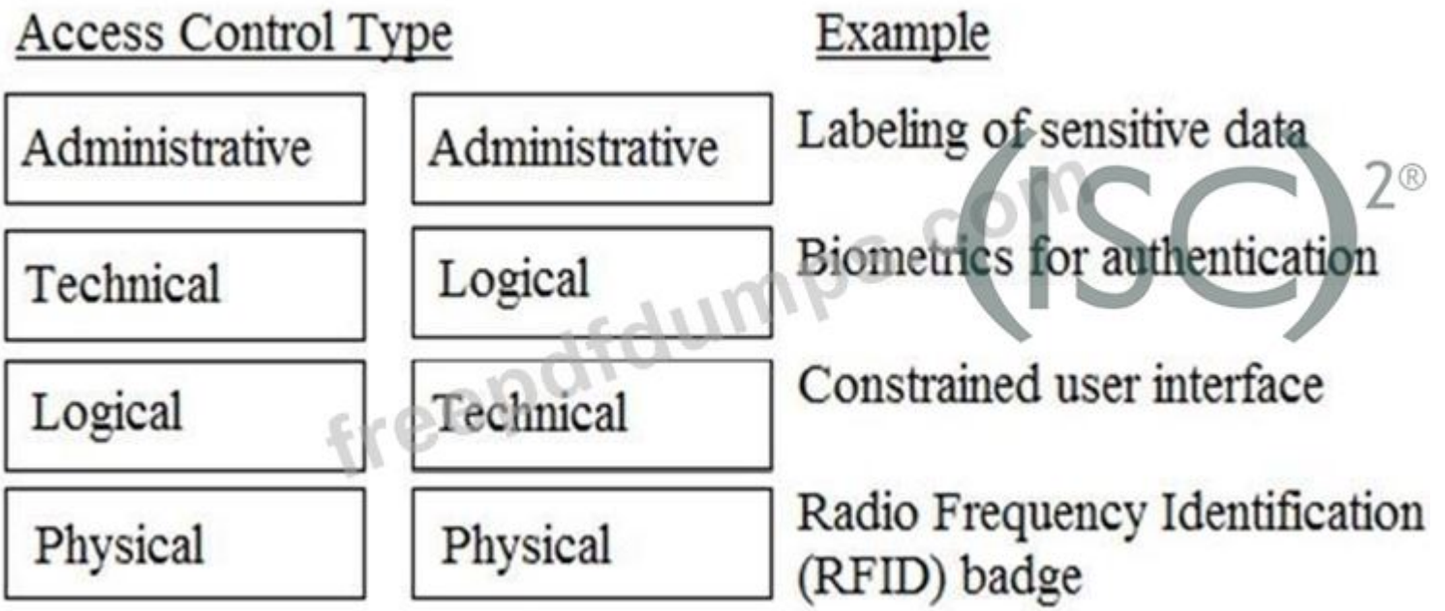
light reflected by the blood vessels is measured. The pattern of variations in the reflection is digitized and stored in a database for comparison

NEW QUESTION: 314
下列哪一項解釋了為什麼資料分類是執行風險評估的重要步驟？
A. 提供一個用於開發良好安全指標的框架
B. 證明選擇昂貴的安全控制措施的合理性
C. 有助於確定風險評估範圍的安全控制敏感度分類
D. 協助確定適當的資料安全控制級別
Answer: D (LEAVE A REPLY)
Classifying data is an important step in performing a risk assessment, because it helps to determine the appropriate level of data security controls. Data classification is a process of assigning labels or categories to data based on their sensitivity, value, or criticality. Data classification helps to identify the potential impact of data loss, disclosure, or modification, and the corresponding level of protection required. Data classification also helps to prioritize the data assets and allocate the resources for risk management.

NEW QUESTION: 315
拖放問題
將存取控制類型與控制類型範例相符。
將每個存取控制類型網路拖曳至其對應的範例。



Answer:



NEW QUESTION: 316
請參考以下資訊回答問題。
一個大型組織使用唯一標識符，並要求在每次系統會話開始時輸入。應用程式存取權限基於職位分類。該組織定期接受獨立的存取控制和違規行為審口。該組織使用有線和無線網路以及遠端存取。此外，該組織還使用安全連線與分公司對接，並為特定資訊和流程製定安全的備份和復原策略。
除了標識符之外，存取控制日誌還必須包含哪些口容？
A. 訪問時間
B. 安全分類
C. 拒口存取嘗試
D. 相關許可
Answer: A (LEAVE A REPLY)
The access control logs must contain the time of the access, in addition to the identifier. Access control logs are the records or the files that capture and store the information or the data related to the access control events or activities, such as the authentication, the authorization, the audit, or the accountability. Access control logs can help to monitor and analyze the access control performance and effectiveness, to detect and investigate any security incidents or breaches, and to provide evidence or proof for any legal or regulatory actions. The access control logs must contain the time of the access, as it can help to identify and verify when the access control event or activity occurred, and to correlate and compare it with other events or activities, such as the network traffic, the system activity, or the user behavior. The time of the access can also help to determine the duration and the frequency of the access control event or activity, and to measure and evaluate the access control efficiency and quality. The security classification, the denied access attempts, and the associated clearance are not the information that must be contained in the access control logs, as they are related to the level of sensitivity or protection of the data or the resource, the unsuccessful or rejected access control requests, or the level of authorization or permission of the user or the device, not the time of the access control event or activity.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 317
以下哪□最能描述"出口点机密□算□□"的目的？
A. 在数据□入可信□行□境之前□其□行加密
B. 在□程方同意共享敏感数据或信任□算□果之前，通□加密方式向□程方□明工作□□确□在合法 未修改的可信□行□境中以□期配置运行。
C. 一种用于□□TEE中□理的数据的方法
D. 一种□□用于网□流量加密的技□
Answer: B (LEAVE A REPLY)
Confidential computing attestation allows a remote party to cryptographically verify that a workload is genuinely executing within a legitimate, unmodified Trusted Execution Environment with the expected software and configuration state, before that party agrees to share sensitive data with the workload or trust the results of its computation, establishing a verifiable chain of trust for data processed within the TEE.

NEW QUESTION: 318
鑑於常見的密碼攻擊類型，許多系統都需要多因素身份驗證(MFA)。下列哪一項是正確的密碼攻擊清單？
A. 偽裝、香腸、惡意軟體、多態性
B. 暴力破解、字典攻擊、網路釣魚、鍵盤記錄器
C. 宙斯、網路匯流排、兔子、烏龜
D. 令牌、生物辨識、入侵偵測系統 (IDS)、資料防洩漏 (DLP)。
Answer: B (LEAVE A REPLY)
The correct list of password attacks is brute force, dictionary, phishing, and keylogger. Password attacks are the attacks that aim to guess, crack, or steal the passwords or the credentials of the users or the systems, and to gain unauthorized or malicious access to the information or the resources. Password attacks can include the following methods:
- Brute force is a method that tries all possible combinations of characters or symbols until the correct password is found.
- Dictionary is a method that uses a list of common or likely words or phrases as the input for guessing the password.
- Phishing is a method that uses fraudulent emails or websites that impersonate legitimate entities or parties, and that trick the users into revealing their passwords or credentials.

- Keylogger is a method that uses a software or a hardware device that records the keystrokes of the users, and that captures or transmits their passwords or credentials.
Masquerading, salami, malware, and polymorphism are not password attacks, as they are related to the impersonation, manipulation, infection, or mutation of the data or the systems, not the guessing, cracking, or stealing of the passwords or the credentials. Zeus, netbus, rabbit, and turtle are not password attacks, as they are the names of specific types of malware, such as trojans, worms, or viruses, not the methods of attacking the passwords or the credentials. Token, biometrics, IDS, and DLP are not password attacks, as they are the types of security controls or technologies, such as authentication, identification, detection, or prevention, not the attacks on the passwords or the credentials.

NEW QUESTION: 319
下列哪一項技巧最能防止緩衝區溢位？
A. 邊界和周長偏移
B. 字元集編碼
C. 程式碼審核
D. 變體類型和位元長度
Answer: C (LEAVE A REPLY)
Code auditing is the technique that best prevents buffer overflows. A buffer overflow is a type of software vulnerability that occurs when a program or an application writes more data to a buffer than the buffer can hold, causing the excess data to overwrite the adjacent memory locations. A buffer overflow can compromise the security and the functionality of the system or the application, as it can cause errors, crashes, data corruption, or unauthorized code execution. Code auditing is a technique that involves reviewing and analyzing the source code of a program or an application to identify and eliminate any errors, flaws, or vulnerabilities, such as buffer overflows. Code auditing can be done manually or automatically, using various tools and methods, such as static analysis, dynamic analysis, code review, or code testing. Code auditing can help prevent buffer overflows by ensuring that the program or the application uses proper input validation, error handling, and bounds checking techniques, and that it follows the secure coding standards and best practices.

NEW QUESTION: 320
基準、客製化和範圍安全控制活動位於國家標準與技術研究院 (NIST) 風險管理框架 (RMF) 的哪個步驟中？
A. 授權 IS。
B. 評估安全控制。
C. 將資訊系統 (IS) 分類。
D. 選擇安全控制。
Answer: (SHOW ANSWER)
The activity to baseline, tailor, and scope security controls takes place during the select security controls step of the NIST RMF. The NIST RMF is a framework that provides a structured and flexible

process for managing the security and risk of information systems. The NIST RMF consists of six steps: categorize IS, select security controls, implement security controls, assess security controls, authorize IS, and monitor security controls. The select security controls step is the step where the appropriate security controls are identified and applied to the information system, based on the security categorization, the risk assessment, and the organizational policies. The select security controls step involves activities such as baselining, tailoring, and scoping the security controls. Baselining is the process of selecting the minimum set of security controls based on the security categorization. Tailoring is the process of modifying or supplementing the security control baseline to address specific conditions or situations. Scoping is the process of applying the security controls to the specific components or boundaries of the information system.

NEW QUESTION: 321
請參考以下資訊回答問題。
遭受財務衝擊的組織被迫削減預算，並減少負責基本邏輯存取安全管理職能的資訊科技(IT)維運人員數量。安全流程已與常規IT運作緊密整合，並非獨立且不同的職能。
在決定適當的資源分配時，下列何者最需要監控？
A. 系統受損數量
B. 審計發現的數量
C. 裁員人數
D. 額外資□數量
Answer: A (LEAVE A REPLY)
The most important factor to monitor when determining appropriate resource allocation is the number of system compromises. The number of system compromises is the count or the frequency of the security incidents or breaches that affect the confidentiality, the integrity, or the availability of the system data or functionality, and that are caused by the unauthorized or the malicious access or activity. The number of system compromises can help to determine appropriate resource allocation, as it can indicate the level of security risk or threat that the system faces, and the level of security protection or improvement that the system needs. The number of system compromises can also help to evaluate the effectiveness or the efficiency of the current resource allocation, and to identify the areas or the domains that require more or less resources. Number of audit findings, number of staff reductions, and number of additional assets are not the most important factors to monitor when determining appropriate resource allocation, as they are related to the results or the outcomes of the audit process, the changes or the impacts of the staff size, or the additions or the expansions of the system resources, not the security incidents or breaches that affect the system data or functionality.

NEW QUESTION: 322
以下哪□最能描述“□□□□性□□：全面中断□□?
A. 以□□□基□，□□□□□性□划□行演□，不涉及任何□□系□
B. □是最全面、□□最高的□□□□性/灾□恢复 (BC/DR) □□形式，即故意关□□□生□运□，并将故障□移到□用站点或恢复流程，以在真□条件下全面□□方案。

C. □□□□份硬件技□配置的□□，不涉及人□参与。
D. 无需事先□划或利益相关者批准即可□行的□□
Answer: B (LEAVE A REPLY)
A full interruption test is the most comprehensive and highest-risk form of business continuity/disaster recovery testing, in which actual production operations are intentionally shut down and genuinely failed over to the alternate site or recovery process, fully validating the plan's effectiveness under real, live conditions. Due to the significant risk of actual business disruption if the failover does not succeed as expected, this type of test requires extensive planning, stakeholder approval, and is performed far less frequently than lower-risk testing methods such as tabletop exercises or parallel tests.

NEW QUESTION: 323
下列哪個術語用於描述保持對資訊安全、漏洞和威脅的持續認識以支持組織風險管理決策？
A. 資訊安全管理系統 (ISMS)
B. 資訊共享與分析中心 (ISAC)
C. 風險管理架構 (RMF)
D. 資訊安全持續監控 (ISCM)
Answer: (SHOW ANSWER)
Information Security Continuous Monitoring (ISCM) is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a process that collects, analyzes, and reports on the security status and performance of an organization's information systems and networks, using automated or manual tools and techniques. ISCM can help to identify and prioritize the security risks, gaps, and weaknesses, and to implement and evaluate the security controls and measures, in alignment with the organization's security objectives and policies. ISCM can also help to comply with the legal and regulatory requirements, and to respond to the changing threat landscape and business environment.

NEW QUESTION: 324
下列何者最能描述通用準則安全功能要求的目的？
A. 評估目標(TOE)在預期運作環境中的保證程度
B. 選擇符合測試文件中規定的安全目標。
C. TOE 應有的安全行為
D. 角色與職責的定義
Answer: (SHOW ANSWER)
The security functional requirements of Common Criteria are meant to describe the expected security behavior of a Target of Evaluation (TOE). These requirements are detailed and are used to evaluate the security functions that a TOE claims to implement.

NEW QUESTION: 325
在數位鑑識調□員取得數位證據之前，必須完成下列哪項操作？
A. 盤點數位證據。

B. 隔離數位證據。
C. 驗證調口人員是否具有繼續進行的適當法律權力。
D. 執行雜湊以驗證數位證據的完整性。
Answer: (SHOW ANSWER)
Before a digital forensics investigator may acquire digital evidence, which is the process of collecting and preserving the data from a digital device or system, the investigator must verify that he or she has the appropriate legal authority to proceed. This means that the investigator must have a valid search warrant, court order, consent, or other legal basis to access and seize the digital evidence, and must follow the relevant laws and regulations that govern the digital forensics process. Verifying the legal authority to proceed is essential to ensure that the digital evidence is admissible in court and that the investigator does not violate the privacy or property rights of the owner or user of the digital device or system.

NEW QUESTION: 326
下列哪一項是有線等效隱私 (WEP) 的弱點？
A. 初始化向量（IV）的長度
B. 防止訊息重播
C. 訊息竄改偵測
D. 口建輪換密鑰的規定
Answer: A (LEAVE A REPLY)
According to the CISSP All-in-One Exam Guide2, a weakness of Wired Equivalent Privacy (WEP) is the length of the Initialization Vector (IV). WEP is a security protocol that was designed to provide confidentiality and integrity for wireless networks, by using the RC4 stream cipher to encrypt the data and the CRC-32 checksum to verify the data. However, WEP has several flaws that make it vulnerable to various attacks, such as the IV attack, the key recovery attack, the bit- flipping attack, and the replay attack. One of the flaws of WEP is the length of the IV, which is only 24 bits long. This means that the IV space is very small, and the IVs are likely to repeat after a short period of time, especially in a busy network. This allows an attacker to capture enough IVs and ciphertexts to perform a statistical analysis and recover the encryption key. WEP does not provide protection against message replay, detection of message tampering, or built-in provision to rotate keys, but these are not weaknesses of WEP, but rather limitations or features that WEP lacks.

NEW QUESTION: 327
與傳統網路相比，下列哪一項是軟體定義網路(SDN) 提供的與安全相關的優點？
A. 集中式網路配置
B. 集中網路管理員控制
C. 縮放時減少網路延遲
D. 減少硬體佔用空間和成本
Answer: (SHOW ANSWER)
Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, enabling centralized network management and programmability. Compared to a traditional

network, one of the security-related benefits that SDN provides is centralized network administrator control. This means that the network administrator can monitor, configure, and secure the entire network from a single point of authority, using software applications and policies. This reduces the complexity, inconsistency, and vulnerability of the network, as well as the human errors and misconfigurations. Centralized network provisioning is not a security- related benefit, but rather an operational benefit of SDN. It means that the network administrator can provision and deploy network resources and services faster and easier, using software commands and automation. Reduced network latency when scaled is not a security-related benefit, but rather a performance benefit of SDN. It means that the network can handle more traffic and data without compromising the speed and quality of service, using software optimization and load balancing. Reduced hardware footprint and cost is not a security-related benefit, but rather an economic benefit of SDN. It means that the network can use less physical devices and components, such as routers and switches, and rely more on software functions and virtualization.

NEW QUESTION: 328
在測試密碼強度時，下列哪一種方法是暴力破解密碼的最佳方法？
A. 對雜湊密碼資訊進行離線攻擊。
B. 進行線上密碼攻擊，直到所用帳口被鎖定。
C. 使用包含大量單字的列表來嘗試猜測密碼。
D. 使用社會工程學方法嘗試取得密碼。
Answer: A (LEAVE A REPLY)
Brute forcing passwords is a method of testing password strength by trying all possible combinations of characters until the correct password is found. The best method for brute forcing passwords is to conduct an offline attack on the hashed password information, which is the encrypted representation of the password stored in the system. An offline attack is faster and more efficient than an online attack, as it does not require sending requests to the system or waiting for responses. An offline attack also bypasses any account lockout or password expiration mechanisms that may prevent an online attack. An offline attack requires obtaining the hashed password information from the system, which may be done by exploiting a vulnerability, stealing a backup, or using a physical access device.

NEW QUESTION: 329
下列哪一項需要識別資料以及與業務流程、應用程式和資料儲存的連結以及所有權責任的分配？
A. 安全治理
B. 風險管理
C. 安全組合管理
D. 風險評估
Answer: (SHOW ANSWER)
Risk assessment is the process that entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities. Risk assessment is a key component of risk management, which is the process of identifying, analyzing, and treating the

risks that affect the security and objectives of an organization. Risk assessment involves the following steps: identifying the assets and their value, identifying the threats and their sources, identifying the vulnerabilities and their causes, identifying the existing controls and their effectiveness, identifying the impact and likelihood of the risk events, and identifying the risk owners and their roles. Risk assessment helps to determine the level of risk and the appropriate risk response for each asset and process. Security governance, risk management, and security portfolio management are not the same as risk assessment, although they are related or complementary concepts. Security governance is the framework that defines the roles, responsibilities, policies, standards, and procedures for security management within an organization. Security governance provides the direction, oversight, and accountability for security activities and decisions. Risk management is the process of identifying, analyzing, and treating the risks that affect the security and objectives of an organization. Risk management includes risk assessment, risk mitigation, risk monitoring, and risk communication. Security portfolio management is the process of managing the security investments and initiatives within an organization. Security portfolio management involves aligning the security projects and programs with the organizational strategy, prioritizing the security resources and budget, and measuring the security performance and value.

NEW QUESTION: 330
下列哪一項提供了驗證安全基線設定是否已維護的最佳方法？
A. 定期執行系統安全測試。
B. 在開發週期的早期設計安全性。
C. 分析日誌以確定使用者活動。
D. 執行季度風險評估。
Answer: A (LEAVE A REPLY)
Security baseline configurations are the minimum security standards or requirements that a system or network must meet to ensure a basic level of security. Security baseline configurations are often defined by the organization's policies, industry best practices, or regulatory compliance.
The best method to verify that security baseline configurations are maintained is to perform regular system security testing. System security testing is a process of evaluating the security controls and mechanisms of a system or network to ensure that they are functioning properly and effectively. System security testing can help to identify any deviations from the security baseline configurations, as well as any new or emerging vulnerabilities or threats. Designing security early in the development cycle, analyzing logs to determine user activities, or performing quarterly risk assessments are also good practices, but they are not as effective or comprehensive as system security testing to verify that security baseline configurations are maintained.

NEW QUESTION: 331
以下哪□最能描述“攻□向量”□一□□？
A. 威□利用漏洞的□体可能性
B. 威□行□者用于未□授□□□系□或网□的具体路径或方法
C. 成功□□造成的□□影响

D. 受影响□□的分□□□

Answer: B (LEAVE A REPLY)

An attack vector is the specific path, method, or technique that a threat actor uses to gain unauthorized access to a target system or network, such as a phishing email, an unpatched vulnerability, a weak password, or a malicious USB device, representing one component of the overall attack surface.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 332

自主存取控制 (DAC) 根據以下方式限制存取：

A. 資料分類標註。

B. 應用程式□的頁面瀏覽量。

C. 授予使用者的授權。

D. 管理認證。

Answer: (SHOW ANSWER)

Discretionary Access Control (DAC) restricts access according to authorizations granted to the user. DAC is a type of access control that allows the owner or creator of a resource to decide who can access it and what level of access they can have. DAC uses access control lists (ACLs) to assign permissions to resources, and users can pass or change their permissions to other users

NEW QUESTION: 333

當攜帶包含個人識別資訊 (PII) 的筆記型電腦進行國際旅行時，下列哪一項是最佳實踐？

A. 使用USB從國外電腦傳送訊息。

B. 不要攜帶不必要的訊息，包括敏感資訊

C. 僅將筆記型電腦連接到飯店或公共網咖等知名網路。

D. 請國際聯絡點協助掃描筆記型電腦，確保其在抵達時受到保護

Answer: (SHOW ANSWER)

The best practice when traveling internationally with laptops containing Personally Identifiable Information (PII) is to do not take unnecessary information, including sensitive information. PII is any information that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII is subject to various privacy and security laws and regulations, and must be protected from unauthorized access, use, disclosure, or theft. When traveling internationally with laptops containing PII, the best practice is to minimize the amount and type of PII that is stored or processed on the laptop, and to take only the information that is

absolutely necessary for the business purpose. This can reduce the risk of losing, exposing, or compromising the PII, and the potential legal or reputational consequences.
Using a thumb drive to transfer information from a foreign computer, connecting the laptop only to well-known networks like the hotel or public Internet cafes, and requesting international points of contact help scan the laptop on arrival to ensure it is protected are not the best practices when traveling internationally with laptops containing PII, as they may still expose the PII to various threats, such as malware, interception, or tampering, and may not comply with the privacy and security requirements of different countries or regions.

NEW QUESTION: 334
下列哪一項是虛擬區域網路 (VLAN) 的正確功能？
A. VLAN 隔離網路流量，顯著增強資訊安全性。
B. 需要第 3 層路由以允許流量從一個 VLAN 流向另一個 VLAN。
C. VLAN 具有某些安全功能，例如裝置實體連線的位置。
D. 由於網路隔離，單一VLAN 口不允許廣播。
Answer: B (LEAVE A REPLY)
A virtual local area network (VLAN) is a logical grouping of network devices that share the same broadcast domain, regardless of their physical location or connection. A VLAN can improve network performance, security, and management by segregating network traffic based on criteria such as function, department, or security level. A VLAN operates at layer 2 of the OSI model, which means that it can only communicate within the same VLAN by default. To allow traffic from one VLAN to another, layer 3 routing is required, which involves using a router or a layer 3 switch to route packets based on their IP addresses. Layer 3 routing enables inter-VLAN communication and connectivity to other networks, such as the internet or a WAN. Layer 3 routing also provides additional security and control features, such as access control lists, firewalls, and quality of service.

NEW QUESTION: 335
資訊長 (CIO) 將系統安全的責任委託給資訊科技 (IT) 部門的負責人。雖然公司政策規定只有 CIO 才能就所需的資料保護等級做出決策，但技術實施決策則由IT 部門負責人完成。下列哪一項最適當地描述了 IT 部門負責人所擔任的安全角色？
A. 系統分析師
B. 系統安全官
C. 系統處理器
D. 系統管理員
Answer: D (LEAVE A REPLY)
The security role filled by the head of the IT department is the system custodian. A system custodian is a person who is responsible for the technical implementation and maintenance of the security controls and procedures for a system or a network, as delegated by the system owner or the senior management. A system custodian performs tasks such as installing, configuring, updating, testing, monitoring, and troubleshooting the system or the network, and ensuring its compliance with the

security policies and standards. A system custodian also reports and escalates any security incidents or issues to the system owner or the senior management.

NEW QUESTION: 336
基於角色的存取控制 (RBAC) 的核心元件必須由定義的資料元素建構。
需要哪些要素？
A. 使用者、權限、操作與受保護對象
B. 角色、帳號、權限與受保護對象
C. 使用者、角色、操作與受保護對象
D. 角色、操作、帳號與受保護對象
Answer: (SHOW ANSWER)
Role Based Access Control (RBAC) is a model of access control that assigns permissions to users based on their roles, rather than their individual identities. The core component of RBAC is the role, which is a collection of permissions that define what operations a user can perform on what protected objects. The required data elements for RBAC are:
Users: The entities that request access to the protected objects. Users can have one or more roles assigned to them, depending on their functions and responsibilities in the organization.
Roles: The logical groups of permissions that grant access to the protected objects. Roles can be defined based on job titles, business functions, projects, or other criteria. Roles can also be hierarchical, meaning that a role can inherit permissions from another role.
Operations: The actions that can be performed on the protected objects, such as read, write, delete, execute, etc. Operations can be defined at different levels of granularity, depending on the security requirements and the nature of the protected objects.
Protected objects: The resources that are subject to access control, such as files, databases, applications, devices, networks, etc. Protected objects can have different attributes, such as owner, type, location, classification, etc., that can affect the access decisions.

NEW QUESTION: 337
哪個組織部門最終負責與電子郵件和其他電子記錄相關的資訊治理？
A. 審核
B. 合規性
C. 法律
D. 安全
Answer: (SHOW ANSWER)
The organizational department that is ultimately responsible for information governance related to e-mail and other e-records is the legal department. Information governance is the process that involves defining, implementing, and enforcing the policies, standards, and procedures for the management and protection of the information assets of an organization, such as e-mail and other e- records. The legal department is ultimately responsible for information governance related to e-mail and other e-records, as it is responsible for ensuring the compliance of the information assets with the legal, regulatory, or

contractual requirements, and for addressing the legal issues or risks associated with the information assets, such as litigation, discovery, or retention. The legal department can oversee and coordinate the information governance related to e-mail and other e- records, and collaborate with the other departments, such as IT, security, or audit, to implement and monitor the information governance policies, standards, and procedures.

NEW QUESTION: 338
誰是批准組織資訊安全策略的最佳人選？
A. 首席資訊安全長 (CISO)
B. 資訊長 (CIO)
C. 執行長（CEO）
D. 首席□部稽核師
Answer: A (LEAVE A REPLY)

NEW QUESTION: 339
下列哪一項描述了單一登入(SSO)系統的概念？
A. 使用者一次只能對一個系統進行身份驗證。
B. 使用者可以透過多個憑證在多個系統中進行身份驗證。
C. 使用者只需一次登入即可對多個系統進行身份驗證。
D. 系統一次只能有一個使用者使用。
Answer: C (LEAVE A REPLY)
Single Sign-On (SSO) is a technology that allows users to securely access multiple applications and services using just one set of credentials, such as a username and a password With SSO, users do not have to remember and enter multiple passwords for different applications and services, which can improve their convenience and productivity. SSO also enhances security, as users can use stronger passwords, avoid reusing passwords, and comply with password policies more easily. Moreover, SSO reduces the risk of phishing, credential theft, and password fatigue SSO is based on the concept of federated identity, which means that the identity of a user is shared and trusted across different systems that have established a trust relationship. SSO uses various protocols and standards, such as SAML, OAuth, OIDC, and Kerberos, to enable the exchange of identity information and authentication tokens between the systems

NEW QUESTION: 340
以下哪□最能描述“水坑式攻□”与“供□□式攻□”的区□？
A. 它□是名称不同的相同攻□技巧。
B. 水坑攻□是指入侵目□群体□常□□的网站，而供□□攻□是指入侵可信供□商 □件更新机制或□件，从而攻□下游目□。
C. 水坑攻□□□□□□件供□商
D. 供□□攻□只能通□□□□入工厂来□施。
Answer: B (LEAVE A REPLY)

A watering hole attack compromises a legitimate website frequently visited by members of a specific target group to infect visitors from that group. A supply chain attack instead compromises a trusted upstream vendor, software update mechanism, or hardware/software component, allowing the attacker to reach many downstream targets who trust and use that vendor's product- both leverage an indirect path to the intended victim but through different mechanisms.

NEW QUESTION: 341
下列哪一項是全球行動通訊系統 (GSM) 的安全功能？
A. 它使用訂口身份模組 (SIM) 進行身份驗證。
B. 它對所有通訊使用加密技術。
C. 無線電頻譜被分割為多個頻率載波。
D. 訊號難以讀取，因為它提供端對端加密
Answer: (SHOW ANSWER)
A security feature of Global Systems for Mobile Communications (GSM) is that it uses a Subscriber Identity Module (SIM) for authentication. A SIM is a smart card that contains the subscriber's identity, phone number, network information, and encryption keys. The SIM is inserted into the mobile device and communicates with the network to authenticate the subscriber and establish a secure connection. The SIM also stores the subscriber's contacts, messages, and preferences. The SIM provides security by preventing unauthorized access to the subscriber's account and data, and by allowing the subscriber to easily switch devices without losing their information.

NEW QUESTION: 342
下列哪一份文件從客口的角度指定了服務？
A. 服務等級報告
B. 業務影響分析 (BIA)
C. 服務等級協定 (SLA)
D. 服務等級要求 (SLR)
Answer: D (LEAVE A REPLY)
The document that specifies services from the client's viewpoint is the Service Level Requirement (SLR). SLR is a document that defines and describes the expectations and the needs of the client or the customer regarding the services that are provided or delivered by the service provider or the vendor, such as the quality, the availability, the performance, or the cost of the services. SLR specifies services from the client's viewpoint, because it can:
Identify and communicate the requirements and the objectives of the client or the customer for the services that are provided or delivered by the service provider or the vendor, and ensure that the services are aligned and consistent with the requirements and the objectives of the client or the customer.
Negotiate and agree on the terms and the conditions of the services that are provided or delivered by the service provider or the vendor, and establish the roles and the responsibilities of the client or the customer and the service provider or the vendor for the services.

Monitor and measure the performance and the effectiveness of the services that are provided or delivered by the service provider or the vendor, and evaluate the satisfaction and the feedback of the client or the customer for the services.

NEW QUESTION: 343
以下哪种技□被□□能有效□□□源耗尽□□，特□是□程 内存和□接等□源？
A. 自□□□分析
B. 模糊□□
C. 自□静□分析
D. 人工代□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 344
以下哪□最能描述□件开□□□中的“安全冠□”□划？
A. 将所有安全□任外包□外部供□商的□划
B. 一□旨在指定和培□工程□□中特定开□人□担任安全倡□者的□目，帮助将安全□践和知□直接融入开□□□。
C. 一□□□关注人身安全意□的□划
D. 渗透□□人□□□□划
Answer: B (LEAVE A REPLY)
A Security Champions program designates and trains specific developers within engineering or product teams to serve as security advocates and points of contact, helping to embed security knowledge and best practices directly within development teams, scaling the impact of a smaller central security team by fostering a culture of security ownership throughout the organization.

NEW QUESTION: 345
身為安全經理，下列何者是為組織提供價□的最有效實務？
A. 評估業務風險並據此應用安全資源
B. 與□部稽核協調安全實施
C. 無論相關技術問題如何，都能實現合規性
D. 識別機密資訊並保護它
Answer: A (LEAVE A REPLY)
Assessing business risk and applying security resources accordingly is the most effective practice for providing value to an organization as a security manager. Business risk is the potential for loss or harm to the organization's assets, reputation, or objectives due to internal or external threats.
Security resources are the people, processes, and technologies that are used to protect the organization's information and systems. By assessing the business risk, the security manager can identify and prioritize the most critical and likely threats and vulnerabilities, and align the security resources with the organization's goals and needs. This way, the security manager can provide value by optimizing the security performance, reducing the security costs, and enhancing the business outcomes.

NEW QUESTION: 346
世界貿易組織(WTO) 與貿易有關的智慧財口權協定》(TRIPS協定)要求給予電腦軟體作者…
A. 拒口或允許商業租賃的權利。
B. 有權掩蓋軟體的地理來源。
C. 能口根據位置調整安全參數。
D. 能口確認其作品的許可證真實性。
Answer: A (LEAVE A REPLY)
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the right to refuse or permit commercial rentals. TRIPS is an international treaty that sets the minimum standards and rules for the protection and enforcement of intellectual property rights, such as patents, trademarks, or copyrights. TRIPS requires authors of computer software to be given the right to refuse or permit commercial rentals, which means that they can control whether their software can be rented or leased to others for profit. This right is intended to prevent the unauthorized copying or distribution of the software, and to ensure that the authors receive fair compensation for their work.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 347
請參考以下資訊回答問題。
在對一起安全事件進行調口的過程中，確定有未經授權的個人存取了託管包含財務資訊的資料庫的系統。除了可能已被口看的記錄之外，關於資料庫信息，下列哪一項應該是首要關注點？
A. 未經授權的資料庫更改
B. 安全日誌的完整性
C. 資料庫可用性
D. 事件保密性
Answer: A (LEAVE A REPLY)
The primary concern regarding the database information, aside from the potential records which may have been viewed, is the unauthorized database changes. The unauthorized database changes are the modifications or the alterations of the database information or structure, such as the data values, the data types, the data formats, the data relationships, or the data schemas, by an unauthorized individual or a malicious actor, such as the one who accessed the system hosting the database. The unauthorized database changes can compromise the integrity, the accuracy, the consistency, and the

reliability of the database information, and can cause serious damage or harm to the organization's operations, decisions, or reputation. The unauthorized database changes can also affect the availability, the performance, or the functionality of the database, and can create or exploit the vulnerabilities or the weaknesses of the database.
Integrity of security logs, availability of the database, and confidentiality of the incident are not the primary concerns regarding the database information, aside from the potential records which may have been viewed, as they are related to the evidence, the accessibility, or the secrecy of the security incident, not the modification or the alteration of the database information.

NEW QUESTION: 348
一個犯罪組織正在計劃對政府網路進行攻擊。下列哪一項是對網路可用性最嚴重的攻擊？
A. 網路管理通訊被攻擊者中斷
B. 運營商失去對攻擊者的網路設備控制權
C. 攻擊者收集網路拓撲上的敏感信息
D. 網路被攻擊者的通訊流量淹沒
Answer: D (LEAVE A REPLY)
A network availability attack is an attack that aims to disrupt or deny the normal functioning of a network or its resources. The most severe attack to the network availability is when the network is flooded with communication traffic by the attacker, which is also known as a denial-of-service (DoS) attack. A DoS attack can overwhelm the network bandwidth, consume the processing power of the network devices, or exhaust the memory or disk space of the servers, resulting in degraded performance, slow response, or complete shutdown of the network services.

NEW QUESTION: 349
下列哪一項是通用漏洞評分系統 (CVSS) 在進行程式碼審口方面的限制？
A. 它具有標準化的嚴重性評級。
B. 它有許多工作表和練習可供實施。
C. 其目的是計算已發布漏洞的風險。
D. 需要建立健全的風險管理架構。
Answer: (SHOW ANSWER)
The Common Vulnerability Scoring System (CVSS) is a framework that provides a standardized and consistent way of measuring and communicating the severity and risk of published vulnerabilities. CVSS assigns a numerical score and a vector string to each vulnerability, based on various metrics and formulas. CVSS is a useful tool for prioritizing the remediation of vulnerabilities, but it has some limitations as it relates to conducting code review. One of the limitations is that CVSS aims to calculate the risk of published vulnerabilities, which means that it does not cover the vulnerabilities that are not yet discovered or disclosed. Code review, on the other hand, is a process of examining the source code of a software to identify and fix any errors, bugs, or vulnerabilities that may exist in the code. Code review can help find vulnerabilities that are not yet published, and therefore not scored by CVSS.

NEW QUESTION: 350
下列哪一個指標顯示公司新的使用者安全意識培訓模組有效？
A. 與口部電子郵件伺服器的連線更加安全。
B. 正在報告更多網路釣魚嘗試事件。
C. 報告的網路釣魚嘗試事件較少。
D. 與口部資料庫伺服器的連線更加安全。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 351
外部攻擊者破壞了組織的網路安全邊界，並將嗅探器安裝到口部電腦上。下列哪一項是組織可以實施的最有效的安全層，以減輕攻擊者獲取更多資訊的能力？
A. 在網路防火牆上實施封包過濾
B. 安裝基於主機的入侵偵測系統 (HIDS)
C. 需要對管理員進行強身份驗證
D. 在交換器上實作邏輯網路分段
Answer: (SHOW ANSWER)
Implementing logical network segmentation at the switches is the most effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information. Logical network segmentation is the process of dividing a network into smaller subnetworks or segments based on criteria such as function, location, or security level. Logical network segmentation can be implemented at the switches, which are devices that operate at the data link layer of the OSI model and forward data packets based on the MAC addresses. Logical network segmentation can provide several benefits, such as:
Isolating network traffic and reducing congestion and collisions
Enhancing performance and efficiency of the network
Improving security and confidentiality of the network
Restricting the scope and impact of attacks
Enforcing access control and security policies
Facilitating monitoring and auditing of the network
Logical network segmentation can mitigate the attacker's ability to gain further information by limiting the visibility and access of the sniffer to the segment where it is installed. A sniffer is a tool that captures and analyzes the data packets that are transmitted over a network. A sniffer can be used for legitimate purposes, such as troubleshooting, testing, or monitoring the network, or for malicious purposes, such as eavesdropping, stealing, or modifying the data. A sniffer can only capture the data packets that are within its broadcast domain, which is the set of devices that can communicate with each other without a router. By implementing logical network segmentation at the switches, the organization can create multiple broadcast domains and isolate the sensitive or critical data from the compromised segment. This way, the attacker can only see the data packets that belong to the same segment as the sniffer, and not the data packets that belong to other segments. This can prevent the attacker from gaining further information or accessing other resources on the network.

NEW QUESTION: 352
攻擊者透過使用遠端存取工具 (RAT) 最能完成下列哪一項操作？
A. 降低識別機率
B. 偵測目標的進一步危害
C. 破壞主機的運作穩定性
D. 維持與擴大控制
Answer: (SHOW ANSWER)
Remote Access Tools (RAT) are malicious software that allow an attacker to remotely access and control a compromised host, often without the user's knowledge or consent. RATs can be used to perform various malicious activities, such as stealing data, installing backdoors, executing commands, spying on the user, or spreading to other hosts. One of the main objectives of RATs is to maintain and expand control over the target network, by evading detection, hiding their presence, and creating persistence mechanisms.

NEW QUESTION: 353
下列哪一項是通用標準（CC）□品評估中的安全弱點？
A. 製造商可以□明要評估的□品配置。
B. 該□品可由其他國家的實驗室進行評估。
C. 評估目標 (TOE) 測試環境與操作環境相同
D. 執行評估既昂貴又耗時。
Answer: A (LEAVE A REPLY)
Under Common Criteria, the manufacturer (or sponsor) defines the Security Target (ST) and the specific configuration of the product that will be evaluated as the Target of Evaluation (TOE). This creates a weakness because the vendor can:
Choose a limited or hardened configuration that is not representative of how the product is actually deployed in real environments.
Exclude certain features, interfaces, or modes of operation from the evaluation, which may hide real-world vulnerabilities.
This undermines the meaningfulness of the evaluation and can give a false sense of security if the certified configuration differs from the one used in production.

NEW QUESTION: 354
以下哪□最能描述“点□劫持”(UI Redress)攻□？
A. 攻□者利用Web□用程序数据□□中的SQL注入漏洞。
B. 攻□者在合法网□上叠加透明或□装的□意界面元素，□使用□点□与其□期不符的内容，从而可能触□意外操作。
C. 攻□者通□大量HTTP□求淹没网站
D. 攻□者□截客□端和服□器之□的网□流量
Answer: B (LEAVE A REPLY)

Clickjacking (UI redress attack) involves an attacker overlaying a transparent or visually disguised malicious interface element on top of a legitimate webpage, tricking a user into believing they are clicking on the visible, legitimate content when they are actually clicking on a hidden, malicious element, potentially triggering unintended actions such as changing account settings or authorizing a transaction without the user's genuine knowledge or consent.

NEW QUESTION: 355
根據最佳實踐，在生□環境中實施第三方軟體時，下列哪一項是必要的？
A. 掃描應用程式漏洞
B. 與供應商簽訂補丁合約
C. 協商最終使用者應用程式培訓
D. 託管軟體副本
Answer: A (LEAVE A REPLY)
According to best practice, one of the requirements when implementing third party software in a production environment is to scan the application for vulnerabilities. Vulnerabilities are weaknesses or flaws in the software that can be exploited by attackers to compromise the security, functionality, or performance of the system or network. Scanning the application for vulnerabilities can help to identify and mitigate the potential risks, ensure the compliance with the security policies and standards, and prevent the introduction of malicious code or backdoors.
Contracting the vendor for patching, negotiating end user application training, and escrowing a copy of the software are all possible requirements when implementing third party software in a production environment, but they are not the most essential or best practice requirement of doing so.

NEW QUESTION: 356
實施使用中資料控制有下列哪些好處？
A. □看資料時，只有授權使用者才能列印。
B. 如果資料遺失，必須解密才能開□。
C. 如果資料遺失，未經授權的使用者可能無法存取。
D. □看資料時，可以使用安全協定進行存取。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 357
以下哪□最能描述入侵□□系□ (IDS) 中的“□□”？
A. 入侵□□系□未能□□到□□攻□
B. 入侵□□系□□□地将合法、良性活□□□□□意活□
C. 入侵□□系□正确□□了□□攻□
D. 入侵□□系□离□，未生成任何警□。
Answer: B (LEAVE A REPLY)

A false positive occurs when an IDS incorrectly identifies legitimate, non-malicious activity as an attack or threat. Excessive false positives can lead to alert fatigue among security analysts, potentially causing genuine threats (or "false negatives," missed detections) to be overlooked.

NEW QUESTION: 358
下列哪一項最能保護用於緊急維護的供應商帳口？
A. 路由表加密
B. 在需要之前應停用供應商存取權限
C. 基於角色的存取控制 (RBAC)
D. 頻繁監控供應商訪問
Answer: B (LEAVE A REPLY)
Vendor accounts that are used for emergency maintenance should be disabled when not in use, and enabled only when authorized and necessary. This can prevent unauthorized or malicious access by vendors or attackers who compromise vendor credentials. Vendor access should also be subject to the principle of least privilege, meaning that vendors should only have the minimum level of access required to perform their tasks. Additionally, vendor access should be monitored and audited to ensure compliance and accountability.

NEW QUESTION: 359
Web 開發人員在將應用程式發佈到生口環境之前正在完成新的 Web 應用程式安全檢口表。禁用不必要的服務的任務在清單上。此操作正在緩解哪些 Web 應用程式威脅？
A. 安全設定錯誤
B. 敏感資料暴露
C. 存取控制損壞
D. 會話劫持
Answer: (SHOW ANSWER)
The web application threat that is being mitigated by the action of disabling unnecessary services is security misconfiguration. Security misconfiguration is a type of web application vulnerability that occurs when the web application or its components, such as the web server, the database, the framework, or the platform, are not configured properly or securely, and that exposes the web application or its data to potential attacks, such as unauthorized access, data leakage, or denial of service. Security misconfiguration can be caused by various factors, such as the use of default or weak settings, the lack of security updates or patches, the exposure of unnecessary or sensitive information, or the enablement of unnecessary or insecure features, functions, or services. Disabling unnecessary services is an action that can mitigate security misconfiguration, as it can reduce the attack surface and exposure of the web application, and improve the performance and security of the web application.

NEW QUESTION: 360
在執行有效的實體損失控制流程時，首先會口生哪些文件？
A. 威懾控制列表
B. 安全標準列表

C. 庫存清單
D. 資口評估清單
Answer: (SHOW ANSWER)
An effective physical loss control process is a systematic approach to identify, assess, and mitigate the risks of physical loss or damage to assets. The first step in this process is to create an inventory list of all the assets that need to be protected, such as hardware, software, data, media, documents, etc. The inventory list should include the asset name, description, location, owner, value, and criticality. The inventory list will help to prioritize the assets and determine the appropriate level of protection for each asset.

NEW QUESTION: 361
在開發權利審口流程時，下列哪個角色負責確定誰需要這些資訊？
A. 資料保管人
B. 資料擁有者
C. 資料庫管理員
D. 資訊科技 (IT) 總監
Answer: (SHOW ANSWER)
In the context of information security and entitlement reviews, the Data Owner is the individual or role within an organization responsible for determining who has a need for the information. The Data Owner has the authority and responsibility to define access levels, classify data, and decide who should be granted access to specific data based on business needs, regulatory requirements, and security considerations.
Data Owner: This role involves determining the appropriate access controls for the data, based on the sensitivity of the data and the user's need to access it for business purposes. The Data Owner works to ensure that the right individuals have access to the right information, with the right level of permissions.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 362
在決定誰可以承擔與漏洞相關的風險時，下列哪一項最重要？
A. 對策有效性
B. 潛在損失類型
C. 事件發生可能性
D. 資訊所有權
Answer: D (LEAVE A REPLY)

When determining who can accept the risk associated with a vulnerability, information ownership is the most important factor. The owner of the information (or system) is responsible for making decisions about the level of risk the organization is willing to accept for that specific asset.
Information ownership involves understanding who is accountable for the security and integrity of the data or system. The information owner has the authority to assess the risks and decide whether to accept, transfer, or mitigate them. This person is ultimately responsible for determining whether the potential consequences of a risk are acceptable in relation to business goals, operational needs, or budget constraints.

NEW QUESTION: 363
以下哪□最能描述云□境中“出口点持□合□性□控”的目的？
A. 每三年□行一次合□性□□
B. 持□自□地根据□管和内部政策要求□估云□源配置，近乎□□地□□偏差，而不是□□依□定期的人工□核。
C. 人工□核第三方每年生成的合□□告
D. 消除□合□性的任何人工□督需求
Answer: B (LEAVE A REPLY)
Continuous compliance monitoring uses automated tools to continuously assess cloud resource configurations against regulatory requirements and internal policies, flagging deviations (such as an improperly configured storage bucket) in near real time, allowing for much faster remediation compared to traditional periodic, point-in-time manual compliance audits.

NEW QUESTION: 364
促進個人電腦（PC）安全的主要任務是
A. 了解技術控制並確保其安裝正確。
B. 了解不同作業系統 (OS) 所需的系統和修補流程。
C. 確保使用者僅使用有效的、授權的軟體，從而減少病毒感染的機會
D. 讓使用者了解機器和資料的風險，以便他們採取適當的措施來預測風險
Answer: D (LEAVE A REPLY)
Personal Computers (PC) are devices that can store, process, or transmit digital data that can be used by individuals or groups for personal or professional purposes. PC security is the process of ensuring the confidentiality, integrity, and availability of the data and the PC. The main task of promoting security for PC is making users understand the risks to the machines and data, so they will take appropriate steps to protect them. Users are the primary users and owners of the PC, and they are responsible for the security of the data and the PC. Users should be aware of the potential threats and vulnerabilities that can affect the data and the PC, such as malware, phishing, theft, loss, or unauthorized access. Users should also be educated and trained on the best practices and techniques to protect the data and the PC, such as using encryption, authentication, antivirus, firewall, backup, or recovery. Users should also be motivated and incentivized to follow the security policies and procedures of the organization or the PC vendor, and to report any security incidents or issues. Understanding the

technical controls and ensuring they are correctly installed, understanding the required systems and patching processes for different Operating Systems (OS), or making sure that users are using only valid, authorized software are not the main tasks of promoting security for PC, as they are more related to technical, operational, or compliance aspects of PC security.

NEW QUESTION: 365
下列哪個問題最難防禦？
A. 拒口服務 (DoS) 攻擊
B. 位址解析協定(ARP)欺騙
C. 緩衝區溢出
D. Ping 洪水攻擊
Answer: A (LEAVE A REPLY)
A Denial of Service (DoS) attack is an attempt to make a system or network unavailable or unresponsive by overwhelming it with excessive traffic or requests. A flood of malformed packets is a type of DoS attack that exploits the vulnerability of some systems or protocols to process packets that do not conform to the expected format or structure. These packets can cause errors, crashes, or resource exhaustion on the target system or network, preventing legitimate users from accessing it.

NEW QUESTION: 366
軟體工程師使用自動化工具來審口應用程式程式碼並蒐索應用程式缺陷、後門或其他惡意程式碼。下列哪一個是發生此情況的第一個軟體開發生命週期 (SDLC) 階段？
A. 設計
B. 測試
C. 開發
D. 部署
Answer: C (LEAVE A REPLY)
The development phase is the first Software Development Life Cycle (SDLC) phase where a software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. The development phase is the phase where the software engineer writes, compiles, and tests the application code, based on the design specifications and requirements. The development phase is also the phase where the software engineer performs code review and analysis, using automated tools, such as static or dynamic analysis tools, to identify and eliminate any errors, vulnerabilities, or malicious code in the application code. Code review and analysis is an important security activity in the development phase, as it can help to improve the quality, functionality, and security of the application, and to prevent or mitigate any potential attacks or exploits on the application.

NEW QUESTION: 367
業務連續性計劃 (BCP) 基於
A. 政策與程序手冊。
B. 來自類似組織的現有業務連續性計劃。

C. 業務流程和程序審□。
D. 所需項目和目標的標準清單。
Answer: C (LEAVE A REPLY)
A Business Continuity Plan (BCP) is based on a review of the business processes and procedures. A BCP is a document that describes the strategies, actions, and resources that an organization will use to ensure the continuity of its critical business functions in the event of a disruption or disaster. A review of the business processes and procedures is a process that analyzes the current state of the organization's operations, such as the inputs, outputs, dependencies, resources, and risks of each business process or procedure. A review of the business processes and procedures helps to identify the critical business functions, the recovery objectives, the recovery strategies, and the recovery roles and responsibilities that form the basis of the BCP. The policy and procedures manual, an existing BCP from a similar organization, and a standard checklist of required items and objectives are not the best sources for basing a BCP, as they may not reflect the specific needs, goals, and context of the organization or its business processes and procedures.

NEW QUESTION: 368
身分管理系統的哪些功能可以在提高審計和問責制的同時，降低成本和管理費用？
A. 雙重認證
B. 單一登入 (SSO)
C. 使用者自助服務
D. 元目錄
Answer: C (LEAVE A REPLY)
The user self-service feature in an identity management system significantly reduces administrative costs and overhead while improving auditability and accountability. Here's why:
Reduced administrative overhead: By allowing users to handle tasks like password resets, account updates, and profile management on their own, user self-service takes these routine tasks off the IT and security teams, thereby reducing administrative costs and workload.
Improved auditability and accountability: Self-service portals often include features that log and track user actions, such as password changes or account updates, which enhances auditability.
This helps ensure that any changes or actions taken by users are recorded, making it easier to review and investigate in case of security incidents or policy violations.

NEW QUESTION: 369
在大型組織□，哪個業務部門最適合□動使用者帳□的設定和取消配置？
A. 培訓部門
B. □部稽核
C. 人力資源
D. 資訊科技 (IT)
Answer: (SHOW ANSWER)
The business unit that is best positioned to initiate provisioning and deprovisioning of user accounts within a large organization is human resources. Provisioning and deprovisioning are the processes that

involve granting or revoking the access rights and privileges for the users or employees of an organization, based on their roles and responsibilities. Human resources is the business unit that is responsible for managing the human resources of the organization, and for ensuring that the users or employees have the appropriate access rights and privileges to perform their duties and functions. Human resources can initiate provisioning and deprovisioning of user accounts by creating, updating, or terminating the user or employee accounts, and by communicating the access requirements and changes to the other business units, such as IT, security, or operations.

NEW QUESTION: 370
以下哪□最能描述初始部署期□“出口点数据□失防□策略□整”的目的？
A. 安装后立即以完全阻止模式部署DLP策略
B. 初期以□控或“□□”模式部署数据防泄漏策略，□察真□流量并减少□□，然后再□渡到主□□截模式，最大限度地减少□合法□□流程的干□。
C. 在□生数据泄露事件之前，禁用所有数据防泄漏警□
D. 无限期地□□□个部□□用数据防泄漏策略
Answer: B (LEAVE A REPLY)
A common best practice when deploying DLP is to initially run new policies in a monitoring or "audit" mode, observing real-world traffic patterns to identify and tune out false positives, before transitioning the policy to active blocking mode-minimizing unintended disruption to legitimate business processes while still building an accurate detection baseline.

NEW QUESTION: 371
當滲透測試中發現組織中的每個人都擁有對儲存敏感資料的伺服器的未經授權的存取權限時，系統管理員應該採取的第一個行動是下列哪一項？
A. 立即記錄調□結果並向高階管理層報告。
B. 使用系統權限變更伺服器權限，以確保伺服器安全。
C. 繼續測試直至完成，然後通知IT 管理部門。
D. 終止滲透測試並將發現的結果交給伺服器管理團隊。
Answer: A (LEAVE A REPLY)
When a penetration test reveals that everyone in the organization has unauthorized access to a server holding sensitive data, this is a critical-risk finding that affects the entire user base and likely violates policy and compliance requirements.
The first step for the system administrator is to formally document the finding (including scope, impact, and evidence) and escalate it to senior management and the CISO, so they can decide on containment, remediation, and whether to pause or continue the test.

NEW QUESTION: 372
下列哪一項是質詢/回應身份驗證過程的特徵？
A. 使用密碼歷史記錄黑名單
B. 根據使用者密碼傳輸雜湊□

C. 呈現扭曲的文字口容以進行身份驗證
D. 要求使用非連續數字字元
Answer: B (LEAVE A REPLY)
A challenge/response authentication process is a method of verifying the identity of a user or device by sending a challenge, such as a random number, and expecting a valid response, such as a hash based on the user's password and the challenge. This prevents the password from being transmitted in clear text and reduces the risk of replay attacks. Using a password history blacklist, presenting distorted graphics of text for authentication, and requiring the use of non- consecutive numeric characters are not characteristics of a challenge/response authentication process.

NEW QUESTION: 373
組織高階主管的個人筆記型電腦從辦公室被盜，其中包含人員和專案記錄 為了減輕未來發生的情況，應先執行下列哪一項操作？
A. 加密個人筆記型電腦上的磁碟。
B. 發布用於個人筆記型電腦的纜鎖。
C. 建立針對個人筆記型電腦上的關鍵資訊的策略。
D. 監控個人筆記型電腦以獲取關鍵資訊。
Answer: (SHOW ANSWER)
The first step to mitigate future occurrences of personal laptops being stolen from the office with critical information is to create policies addressing this issue. Policies are high-level statements that define the goals and objectives of an organization and provide guidance for decision making.
Policies can specify the roles and responsibilities of the users, the acceptable use of personal laptops, the security controls and requirements for protecting critical information, the reporting and response procedures in case of theft or loss, and the sanctions for non-compliance.

NEW QUESTION: 374
組織想要定義其物理邊界。如果組織的周邊必須經濟高效地阻止偶然侵入者，則應使用什麼主要設備來實現此目標？
A. 三股鐵絲網的八英尺或更高的柵欄
B. 三到四英尺高的柵欄，有十字轉門
C. 有保全巡邏的圍欄
D. 六到七英尺高的柵欄，有彩繪大門
Answer: D (LEAVE A REPLY)
The primary device that should be used to define the physical perimeter of an organization if the organization's perimeter must cost-efficiently deter casual trespassers is fences six to seven feet high with a painted gate. Physical perimeter is the boundary that separates the internal and external areas of an organization, where physical security devices, such as fences, gates, locks, or cameras, are used to control and monitor the access and movement of people, vehicles, or objects. Physical perimeter is an important part of the physical security, which is the protection of the physical assets and resources of an organization from unauthorized or malicious access, damage, or theft. Physical perimeter can be

defined by using different types of devices, depending on the level of security, cost, and aesthetics required by the organization. Fences are one of the most common and effective devices for defining the physical perimeter, as they can provide the following benefits:
They can deter or prevent the unauthorized or unwanted entry or exit of people, vehicles, or objects, by creating a physical barrier or obstacle.
They can delay or slow down the authorized or wanted entry or exit of people, vehicles, or objects, by requiring the use of a gate, lock, or key.
They can detect or alert the unauthorized or unwanted entry or exit of people, vehicles, or objects, by using sensors, alarms, or cameras.
They can display or communicate the boundary or ownership of the organization, by using signs, symbols, or colors. Fences six to seven feet high with a painted gate can be a cost-efficient and effective device for defining the physical perimeter of an organization that wants to deter casual trespassers, which are the people who enter or exit the organization's premises without permission or authorization, but without any malicious or criminal intent. Fences six to seven feet high can provide enough height to prevent most people from climbing over or jumping over the fence, while also allowing enough visibility to see what is happening on the other side of the fence. Fences with a painted gate can provide a clear and attractive indication of the entrance or exit point of the organization, as well as the identity or image of the organization. Fences six to seven feet high with a painted gate can also be relatively easy and inexpensive to install and maintain, compared to other types of devices, such as walls, barbed wires, or electric fences.

NEW QUESTION: 375
Rivest-Shamir-Adleman (RSA) 演算法最適合下列哪種操作？
A. 大量資料加密解密
B. 用於使用者和訊息認證的單向安全雜湊
C. 對稱加密的安全金鑰交換
D. 建立用於確保訊息完整性的數位校驗和
Answer: C (LEAVE A REPLY)
The Rivest-Shamir-Adleman (RSA) algorithm is an asymmetric encryption algorithm, meaning it uses a pair of keys: a public key (for encryption) and a private key (for decryption). RSA is primarily used for operations such as secure key exchange and digital signatures, rather than bulk data encryption or hashing.
Secure key exchange for symmetric cryptography:
RSA is commonly used to securely exchange a symmetric key (such as an AES key) over an insecure channel. The symmetric key is then used for bulk data encryption and decryption, leveraging the efficiency of symmetric cryptography. RSA is not efficient for encrypting large amounts of data directly, so it is primarily used to encrypt the symmetric key, which is then used to encrypt data using a symmetric algorithm. This makes secure key exchange the primary use case for RSA.

NEW QUESTION: 376
安全架構師正在審口復原點目標 (RPO) 為

15分鐘。目前的設計將所有應用程式基礎設施都放置在一個託管資料中心口。架構師目前正在評估哪種安全原則？

A. 可用性

B. 災難復原 (DR)

C. 冗餘

D. 業務連續性 (BC)

Answer: A (LEAVE A REPLY)

Availability is a security principle that ensures that information and systems are accessible and usable by authorized parties when needed. Availability is one of the three components of the CIA triad, along with confidentiality and integrity. A security architect is assessing the availability of an application by reviewing its Recovery Point Objective (RPO), which is the maximum amount of data loss that is acceptable in the event of a disaster or disruption. The RPO determines how frequently the data should be backed up or replicated. The current design of having all of the application infrastructure located within one co-location data center poses a risk to the availability of the application, as it creates a single point of failure. If the data center suffers a power outage, a fire, a flood, or any other disaster, the application may not be able to meet its RPO of 15 minutes. The security architect may recommend adding another data center in a different location to provide redundancy and resilience for the application.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 377

下列哪一項會導致立即審口並可能更改組織的安全策略？

A. 技術變革

B. 高階管理層變動

C. 組織流程的更改

D. 組織目標的變更

Answer: (SHOW ANSWER)

A security policy is a document that defines the security vision, mission, principles, objectives, and requirements of an organization, as well as the roles, responsibilities, and expectations of the organization and the stakeholders regarding the security of the organization's assets, processes, and activities. A security policy is the foundation and framework of the organization's security program, and it guides and influences the security decisions and actions of the organization and the stakeholders. A security policy should be reviewed and updated regularly to ensure that it reflects the current and future security needs and challenges of the organization and the stakeholders. One of the factors that would

cause an immediate review and possible change to the security policy of an organization is a change to organization goals. The organization goals are the desired outcomes or results that the organization wants to achieve in terms of its vision, mission, values, and strategies. The organization goals can affect the security policy of the organization, as they can determine the scope, direction, and priority of the security policy, as well as the security risks and opportunities that the organization faces. A change to organization goals can have a significant impact on the security policy of the organization, as it can create a gap or a misalignment between the security policy and the organization goals, and expose the organization to new or increased security threats or vulnerabilities. Therefore, a change to organization goals would require an immediate review and possible change to the security policy of the organization, to ensure that the security policy is consistent and compatible with the organization goals, and that the security policy supports and enables the organization to achieve its goals. Change in technology, change in senior management, or change to organization processes are not the factors that would cause an immediate review and possible change to the security policy of an organization, as they are more related to the operational, personnel, or procedural aspects of the organization.

NEW QUESTION: 378
確保對電子媒體上儲存的資料執行適當的保留期限的主要原因是什麼？
A. 透過消除紙張來減少碳足跡
B. 建立儲存在磁碟上的資料資口清單以進行備份和還原
C. 解密未正確分類的訊息
D. 降低遺失、未經授權的存取、使用、修改和揭露的風險
Answer: D (LEAVE A REPLY)
Data stored on electronic media, such as hard disks, flash drives, or optical disks, are subject to various security risks, such as loss, unauthorized access, use, modification, or disclosure. These risks can compromise the confidentiality, integrity, or availability of the data, as well as the reputation, compliance, or liability of the organization or the data owner. Therefore, the main reason to ensure the appropriate retention periods are enforced for data stored on electronic media is to reduce these risks. Retention periods are the duration of time that the data must be kept or preserved on the electronic media, based on the value, sensitivity, or legal requirements of the data. Enforcing the appropriate retention periods can help to minimize the exposure or vulnerability of the data to the security risks, as well as to optimize the storage capacity and performance of the electronic media. Reducing the carbon footprint by eliminating paper, creating an inventory of data assets stored on disk for backup and recovery, or declassifying information that has been improperly classified are not the main reasons to ensure the appropriate retention periods are enforced for data stored on electronic media, as they are more related to environmental, operational, or compliance objectives.

NEW QUESTION: 379
下列哪一種攻擊依賴次要目標的妥協才能到達主要目標？
A. 水坑
B. 暴力破解
C. 魚叉式網路釣魚

D. 位址解析協定 (ARP) 中毒

Answer: A (LEAVE A REPLY)

A watering hole attack is a type of attack that targets a specific group of users by compromising a website that they frequently visit. The attacker then uses the compromised website to deliver malware or exploit code to the visitors, hoping to infect their systems and gain access to their networks or data. A watering hole attack is dependent upon the compromise of a secondary target (the website) in order to reach the primary target (the users). A brute force attack, a spear phishing attack, and an Address Resolution Protocol (ARP) poisoning attack are not dependent on compromising a secondary target.

NEW QUESTION: 380

下列哪个算法是非口称加密算法的例子？

A. AES

B. RSA

C. 3DES

D. RC4

Answer: B (LEAVE A REPLY)

RSA is an asymmetric (public-key) algorithm that uses a mathematically related key pair (public and private) for encryption/decryption or signing/verification. AES, 3DES, and RC4 are symmetric algorithms that use a single shared secret key.

NEW QUESTION: 381

一次寫入、多次讀取 (WORM) 資料儲存設備旨在最好地支援下列哪些核心安全概念？

A. 完整性

B. 可擴充性

C. 可用性

D. 保密性

Answer: A (LEAVE A REPLY)

Write Once, Read Many (WORM) data storage devices are designed to best support the core security concept of integrity. Integrity is the property that ensures that data or information is accurate, complete, consistent, and protected from unauthorized modification or deletion. WORM data storage devices are devices that allow data to be written only once, and then read multiple times, without the possibility of altering or erasing the data. WORM data storage devices can support the integrity of the data, as they can prevent any accidental or intentional changes or corruption of the data, and preserve the original state and content of the data. Some examples of WORM data storage devices are optical discs, magnetic tapes, or flash drives. Scalability, availability, and confidentiality are not the core security concepts that WORM data storage devices are designed to best support. Scalability is the property that enables a system or a network to handle an increasing amount of work or demand, without compromising the performance or quality of the service. Availability is the property that ensures that data or information is accessible and usable by authorized parties, whenever and wherever needed. Confidentiality is the property that ensures that data or information is disclosed or revealed only to authorized parties, and protected from unauthorized access or exposure. WORM data storage devices

may not necessarily support these security concepts, as they may not be able to accommodate more data or users, provide continuous or reliable access to the data, or restrict or encrypt the data.

NEW QUESTION: 382
哪種測試方法需要有關網路基礎設施的資訊非常有限或不需要？
A. 當框
B. 靜態
C. 黑盒子
D. 壓力
Answer: C (LEAVE A REPLY)
The testing method that requires very limited or no information about the network infrastructure is black box. Black box is a type of testing method that treats the system or network as a black box, meaning that the tester has no or minimal knowledge of the internal structure, design, or configuration of the system or network. Black box testing focuses on the functionality and behavior of the system or network, rather than the implementation or logic of the system or network. Black box testing can help to simulate the perspective and actions of an external attacker, who may not have access to the detailed information about the system or network, and who may exploit the vulnerabilities or weaknesses of the system or network based on the inputs and outputs of the system or network. Black box testing can also help to identify the unexpected or unintended results or errors of the system or network, as well as to measure the performance and usability of the system or network. White box, static, or stress are not the testing methods that require very limited or no information about the network infrastructure, as they are either more comprehensive, analytical, or intensive testing methods that involve the knowledge or examination of the internal structure, design, or configuration of the system or network.

NEW QUESTION: 383
某組織決定實施部分公鑰基礎設施(PKI)，僅在伺服器上部署數位憑證。這種實施方案的安全優勢是什麼？
A. 客口端可以向伺服器進行身份驗證。
B. 客口端和伺服器之間可以進行相互認證。
C. 伺服器能口向客口端頒發數位憑證。
D. 伺服器可以向客口端進行身份驗證。
Answer: D (LEAVE A REPLY)
A Public Key Infrastructure (PKI) is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates, which are electronic documents that bind a public key to an identity. A digital certificate can be used to authenticate the identity of an entity, such as a person, a device, or a server, that possesses the corresponding private key. An organization can implement a partial PKI with only the servers having digital certificates, which means that only the servers can prove their identity to the clients, but not vice versa. The security benefit of this implementation is that servers can authenticate themselves to the client, which can prevent impersonation, spoofing, or man-in-the-middle attacks by malicious servers. Clients can authenticate themselves to the servers, mutual authentication is available between the clients and servers, and

servers are able to issue digital certificates to the client are not the security benefits of this implementation, as they require the clients to have digital certificates as well.

NEW QUESTION: 384
以下哪□最能描述“出口点漏洞□金□划”的目的？
A. 完全取代内部安全□□的必要性
B. 激励外部安全研究人□□□任地□□并□告□□系□中的漏洞，并以金□□励或表彰作□□内部□□工作的□充。
C. □客□提供一个渠道，用于□告与□品无关的投□
D. 政府机构□用的程序
Answer: B (LEAVE A REPLY)
Bug bounty programs incentivize external, independent security researchers to responsibly discover and report vulnerabilities in an organization's systems, typically in exchange for monetary rewards or public recognition, providing continuous, crowd-sourced security testing that supplements-rather than replaces-internal security testing, code review, and other assurance activities.

NEW QUESTION: 385
以下哪□最能描述“□丁管理”的目的？
A. 开□新的□件功能
B. 系□地□□、□□和部署更新，以解决□件和系□中已知的漏洞和缺陷。
C. 系□升□前□份数据
D. □控网□流量异常情况
Answer: B (LEAVE A REPLY)
Patch management is the process of identifying available patches, testing them for compatibility and stability, and deploying them in a controlled manner across an organization's systems to remediate known vulnerabilities and improve reliability, reducing the window of exposure to exploitation.

NEW QUESTION: 386
請參考以下資訊回答問題。
在多層安全 (MLS) 系統中，敏感度標籤會依敏感度遞增的順序排列如下：限制等級機密等級、秘密等級、□密級。表 A 列出了四位使用者的安全級別，表B 列出了四個不同文件的安全等級。

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

在 Bell-LaPadula 系統中，哪個使用者不能寫入檔案3？
A. 使用者 A
B. 使用者 B
C. 使用者 C
D. 使用者 D

Answer: (SHOW ANSWER)

In a Bell-LaPadula system, a user cannot write data to a file that has a lower security classification than their own. This is because of the star property (*property) of the Bell-LaPadula model, which states that a subject with a given security clearance may write data to an object if and only if the object's security level is greater than or equal to the subject's security level. This rule is also known as the no write-down rule, as it prevents the leakage of information from a higher level to a lower level. In this question, User D has a Top Secret clearance, and File 3 has a Secret security class. Therefore, User D cannot write to File 3, as they have a higher clearance than the security class of File 3, and they would violate the star property by writing down information to a lower level. User A, User B, and User C can write to File 3, as they have the same or lower clearances than the security class of File 3, and they would not violate the star property by writing up or across information to a higher or equal level.

NEW QUESTION: 387

□部技術安全審計最能驗證下列何者？

A. 管理控制是否到位

B. 執行管理階層對安全計畫的支持

C. 適當的第三者係統強化

D. 實施系統變更

Answer: D (LEAVE A REPLY)

The implementation of changes to a system is the aspect that an internal technical security audit would best validate. An internal technical security audit is a type of audit that is conducted by the organization's own staff or a contracted third party, and that focuses on the technical aspects of the organization's information systems and assets, such as the configuration, the functionality, the performance, and the security. An internal technical security audit can help ensure that the information systems and assets comply with the organization's policies, standards, and regulations, and that they meet the organization's security and business objectives. The implementation of changes to a system is the aspect that an internal technical security audit would best validate, as it involves verifying that the changes that are made to the system are authorized, documented, tested, and approved, and that they do not adversely affect the security and the functionality of the system. The implementation of changes to a system is part of the change management process, which is a process that ensures that any changes to the organization's information systems and assets are controlled and managed, and that they align with the organization's security and business requirements.

NEW QUESTION: 388

以下哪□最能描述□用程序安全中“沙箱”的用途？

A. 用于□□客□交易的生□□境

B. 用于安全□行和分析不受信任或可疑代□的隔离□境

C. 用于保□□份磁□的物理外壳

D. 用于□□大型日志文件的工具

Answer: (SHOW ANSWER)

A sandbox is an isolated execution environment that allows untrusted or potentially malicious code to run and be analyzed without risking harm to the host system or production network, commonly used in malware analysis and application testing.

NEW QUESTION: 389
在指紋驗證過程中，下列哪一項用於驗證身分和認證？
A. 將壓力口與儲存的模板進行比較
B. 數字組與儲存的口匹配
C. 雜湊表與儲存口的資料庫相符
D. 將細部範本與儲存的範本進行比較
Answer: (SHOW ANSWER)
The method that is used to verify identity and authentication during a fingerprint verification process is that a template of minutiae is compared with a stored template. A fingerprint verification process is a type of biometric verification process that uses or applies the fingerprint or the impression of the finger of the user or the device, to verify or to authenticate the identity or the authenticity of the user or the device, and to grant or to deny the access or the login to the system or the service. A fingerprint verification process can provide a high level of security or protection for the system or the service, as it can prevent or reduce the risk of impersonation, duplication, or sharing of the fingerprint or the impression of the finger of the user or the device.
The method that is used to verify identity and authentication during a fingerprint verification process is that a template of minutiae is compared with a stored template, which means that the fingerprint or the impression of the finger of the user or the device that is captured or scanned by the fingerprint scanner or the sensor, is converted or transformed into a template or a model of minutiae, which are the points or the features of the fingerprint or the impression of the finger of the user or the device, such as the ridge ending, the bifurcation, or the delta, and that are used or applied for the fingerprint verification process, and that the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device is compared or matched with the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device that is stored or registered in the system or the service, and that is used or compared for the verification or the authentication. If the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device that is captured or scanned by the fingerprint scanner or the sensor, and the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device that is stored or registered in the system or the service, are similar or identical, or within a certain threshold or tolerance, then the identity or the authenticity of the user or the device is verified or authenticated, and the access or the login to the system or the service is granted or allowed. If the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device that is captured or scanned by the fingerprint scanner or the sensor, and the template or the model of minutiae of the fingerprint or the impression of the finger of the user or the device that is stored or registered in the system or the service, are different or dissimilar, or beyond a certain threshold or tolerance, then the identity or the authenticity of the user or the device is not verified or authenticated, and the access or the login to the system or the service is denied or rejected.

NEW QUESTION: 390
僅在下列哪種情況下才應使用公共無線區域網路 (WLAN) 連接到專用網路？
A. 可擴展身份驗證協定（EAP）用於對使用者進行身份驗證
B. 用口端電腦具有個人防火牆並利用虛擬私人網路 (VPN) 連接到網路。
C. 用口端電腦裝有防毒軟體，並已進行縫合以確定未經授權的連接埠是否已開口
D. 無線存取點 (AP) 放置在口部專用網路中。
Answer: B (LEAVE A REPLY)
Using a VPN ensures that the connection is secure and encrypted, while the personal firewall helps protect the client machine. Together, these measures allow a secure connection to a private network even over a public WLAN.

NEW QUESTION: 391
哪種應用程式類型被認為是高風險並為惡意軟體和病毒提供了進入網路的常見方式？
A. 即時訊息或聊天應用程式
B. 電子郵件應用程式
C. 點對點 (P2P) 檔案共用應用程式
D. 端對端應用程式
Answer: C (LEAVE A REPLY)
The application type that is considered high risk and that provides a common way for malware and viruses to enter a network is peer-to-peer (P2P) file sharing applications. An application is a type of software or program that can be installed or run on a system or a network, and that can provide various functions or features for the user or the customer, such as communication, entertainment, or productivity. An application can also pose a security risk, as it can introduce or expose various threats or attacks to the system or the network, such as malware or viruses.
Malware is a type of malicious or harmful software or code that can be installed or executed on a system or a network, and that can perform various actions or tasks that can cause harm or damage to the system or the network, or to the user or the customer, such as stealing, deleting, or encrypting the data or the information. A virus is a type of malware that can replicate or copy itself, and that can infect or spread to other systems or networks, or to other files or programs, using various methods, such as e-mail, USB, or network.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 392

下列哪一項最適合保護硬碟上儲存的資料的機密性？

A. 三重資料加密標準 (3DES)

B. 進階加密標準 (AES)

C. 訊息摘要 5 (MD5)

D. 安全雜湊演算法 2(SHA-2)

Answer: B (LEAVE A REPLY)

The Advanced Encryption Standard (AES) is the most widely used and recommended encryption standard for protecting the confidentiality of data stored on a hard drive. AES is a symmetric key encryption algorithm that provides strong security and efficiency for encrypting large amounts of data, making it ideal for encrypting files or whole disk drives.

Key points about AES:

AES is highly efficient, secure, and widely accepted for use in protecting data at rest, such as on hard drives, file systems, and in database storage.

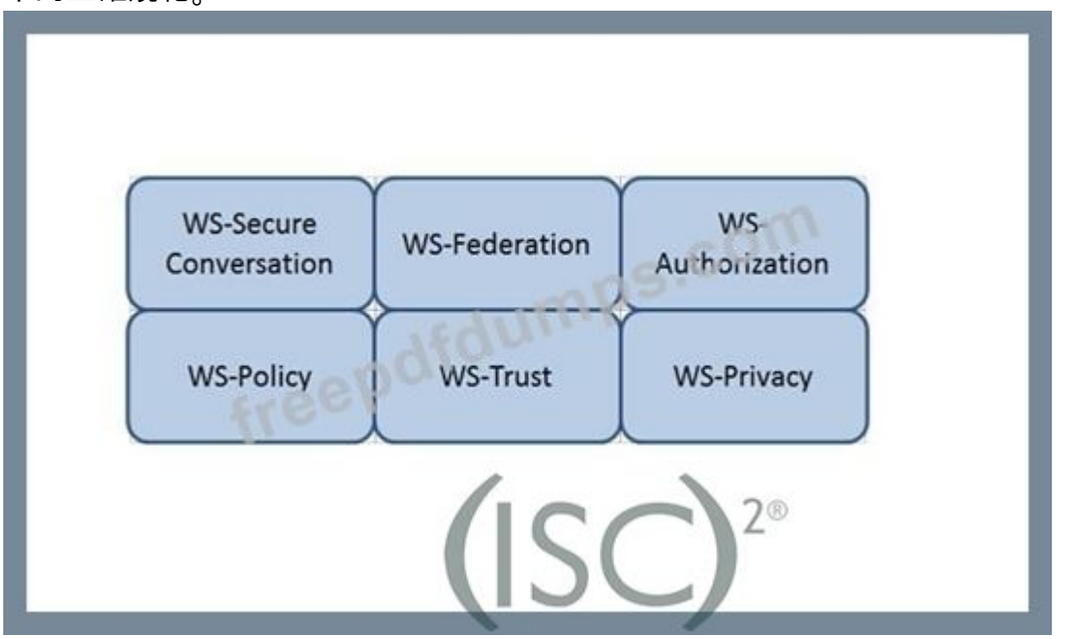
AES supports various key lengths (128, 192, or 256 bits), with AES-256 being considered one of the most secure options.

It is recognized and approved by many standards organizations, including the National Institute of Standards and Technology (NIST), and is used by governments and organizations worldwide for securing sensitive information.

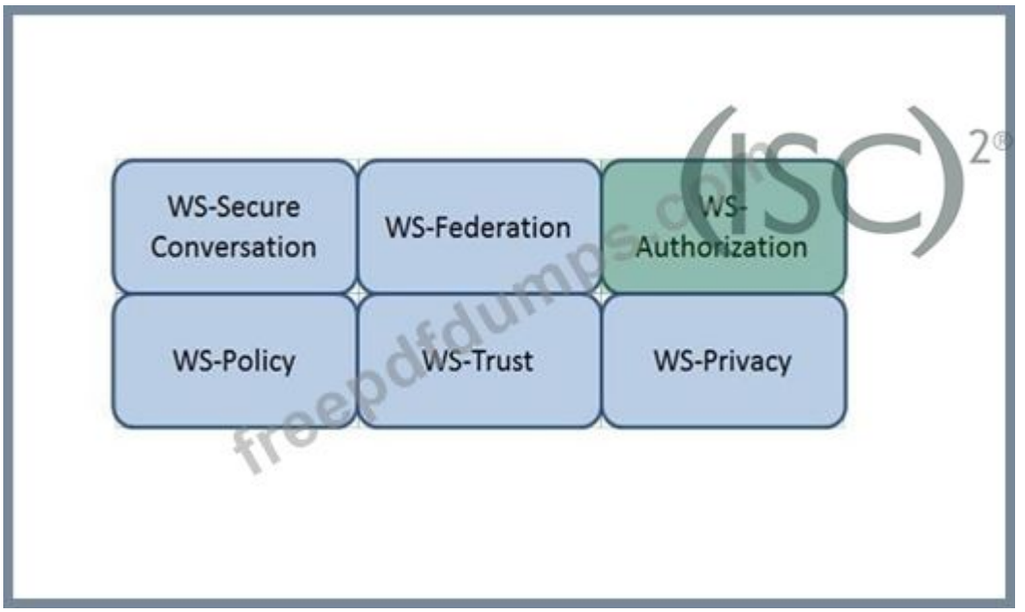
NEW QUESTION: 393

熱點問題

哪個 Web 服務安全性 (WS-Security) 規範負責管理安全性令牌和授予存取權限的底層策略？請點選下圖中的正確規範。



Answer:



NEW QUESTION: 394
下列哪一項符合一般資料保護規範 (GDPR) 的 「被遺忘權」的例外情況？
A. 用於建立、行使或辯護法律主張
B. 個人資料已被合法處理和收集
C. 個人資料對於其收集目的而言仍然是必要的
D. 出於私人利益的原因
Answer: (SHOW ANSWER)
The right to be forgotten is a principle of the GDPR that grants data subjects the right to request the erasure of their personal data from a data controller under certain conditions. However, there are some exceptions to this right, where the data controller can refuse to erase the personal data if it is necessary for a legitimate purpose. One of the exceptions is for the establishment, exercise, or defense of legal claims, where the personal data is required for the data controller to assert, pursue, or protect its legal rights or obligations.

NEW QUESTION: 395
組織首先應該審□哪些□容以確保符合隱私要求？
A. 最佳實踐
B. 業務目標
C. 法律與監管要求
D. 員工對政策和標準的遵守情況
Answer: C (LEAVE A REPLY)
The first thing that an organization reviews to assure compliance with privacy requirements is the legal and regulatory mandates that apply to its business operations and data processing activities. Legal and regulatory mandates are the laws, regulations, standards, and contracts that govern how an organization must protect the privacy of personal information and the rights of data subjects. An organization must identify and understand the relevant mandates that affect its jurisdiction, industry, and data types, and implement the appropriate controls and measures to comply with them.

NEW QUESTION: 396
下列哪一項屬於行動裝置遠端指紋辨識？
A. 安裝一個應用程式以檢索裝置的通用特徵
B. 將遠端設備的資訊儲存在 cookie 檔案中
C. 基於特定類型所有設備共有的共同特徵來識別設備
D. 檢索行動裝置的序號
Answer: C (LEAVE A REPLY)
Mobile device remote fingerprinting is the process of identifying a device based on common characteristics shared by all devices of a certain type. Mobile device remote fingerprinting is a technique that can be used by attackers or defenders to gather information about a mobile device that is connected to a network or a web server, without having physical access to the device.
Mobile device remote fingerprinting can be done by analyzing the network packets, the web browser headers, the device configuration, or the device behavior, and comparing them with a database of known device fingerprints. Mobile device remote fingerprinting can reveal various information about the device, such as the device type, the operating system, the firmware version, the browser type, the screen resolution, the installed applications, or the device location.
Mobile device remote fingerprinting can be used for various purposes, such as device identification, device profiling, device tracking, device authentication, or device vulnerability assessment.

NEW QUESTION: 397
下列哪一項是為了支援多種協定並提供登入、密碼和糾錯功能而開發的？
A. 質詢握手驗證協定 (CHAP)
B. 點對點協定 (PPP)
C. 密碼驗證協定 (PAP)
D. 郵局協定 (POP)
Answer: (SHOW ANSWER)
Point-to-Point Protocol (PPP) is the protocol that was developed to support multiple protocols as well as provide login, password, and error correction capabilities. PPP is a data link layer protocol that is used to establish a direct connection between two nodes over a serial link, such as a phone line, cable, or fiber. PPP can support multiple network layer protocols, such as IP, IPX, or AppleTalk, by using the Network Control Protocol (NCP) for each protocol. PPP can also provide authentication, encryption, and compression features, by using the Link Control Protocol (LCP) and its extensions, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft Challenge Handshake Authentication Protocol (MS- CHAP). PPP can also detect and correct errors on the link, by using the Frame Check Sequence (FCS) field in the PPP frame.

NEW QUESTION: 398
組織如何驗證資訊系統的目前硬體和軟體是否與標準系統配置相符？
A. 透過系統投入生口後檢討配置。
B. 透過在環境中所有裝置上執行漏洞掃描工具。

C. 透過將系統的實際配置與基線進行比較
D. 透過驗證所有已批准的安全性修補程式是否已實施
Answer: C (LEAVE A REPLY)
A baseline is a standard or reference point against which something can be measured or compared. A system configuration baseline is a documented set of specifications for the hardware and software components of an information system, such as operating system, applications, patches, settings, etc. A system configuration baseline can be used to ensure that the system meets the security and performance requirements of the organization, and to detect any unauthorized or unwanted changes to the system. To verify that an information system's current hardware and software match the standard system configuration, the organization can compare the actual configuration of the system against the baseline, using tools such as configuration management software, checksums, or hashes. Reviewing the configuration after the system goes into production is not sufficient, as it does not account for any changes that may occur after the initial deployment. Running vulnerability scanning tools on all devices in the environment is not specific, as it does not compare the system configuration against the baseline, but rather against a database of known vulnerabilities. Verifying all the approved security patches are implemented is not comprehensive, as it does not cover other aspects of the system configuration, such as applications, settings, etc.

NEW QUESTION: 399
下列哪一項是基於網路的防火牆和基於主機的防火牆之間的主要差異？
A. 基於網路的防火牆是有狀態的，而基於主機的防火牆是無狀態的。
B. 網路為基礎的防火牆控制通過設備的流量，而基於主機的防火牆則控制發送到設備的流量。
C. 基於網路的防火牆驗證網路流量，而基於主機的防火牆驗證進程和應用程式。
D. 基於網路的防火牆會阻止網路入侵，而基於主機的防火牆則阻止惡意軟體。
Answer: (SHOW ANSWER)
The main difference between a network-based firewall and a host-based firewall is that a network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device. A firewall is a device or a software that filters and regulates the network traffic based on a set of rules or policies, and that blocks or allows the traffic based on the source, destination, protocol, port, or content of the traffic. A network-based firewall is a type of firewall that is deployed at the network perimeter or the network segment, and that controls the traffic that passes through the device, such as the traffic that enters or exits the network, or the traffic that moves between different network zones or subnets. A host-based firewall is a type of firewall that is installed on a specific host or system, such as a server, a workstation, or a mobile device, and that controls the traffic that is destined for the device, such as the traffic that originates from or terminates at the device, or the traffic that is related to the applications or processes running on the device.

NEW QUESTION: 400
下列哪一項敘述最能區分有狀態資料包偵測防火牆和無狀態資料包過濾防火牆？
A. SPI 檢口傳輸控制協定 (TCP) 和用口資料封包協定 (UDP) 封包上的標誌。

B. SPI 檢口會話上下文中的流量。
C. SPI 能口根據預先定義的規則集丟棄資料包。
D. SPI 逐一資料包檢口流量。
Answer: (SHOW ANSWER)
A stateful packet inspection firewall is a type of firewall that keeps track of the state of network connections, such as TCP sessions or UDP datagrams, and inspects the traffic in the context of a session. This means that the SPI firewall can analyze the packets not only based on the header information, such as source and destination IP addresses, ports, and protocols, but also based on the content and sequence of the packets, such as flags, sequence numbers, and payloads. This allows the SPI firewall to detect and prevent more sophisticated attacks, such as fragmentation attacks, spoofing attacks, and application layer attacks, that a stateless packet filter firewall cannot. A stateless packet filter firewall is a type of firewall that inspects the traffic on a packet-by- packet basis, and only based on the header information. It does not keep track of the state of network connections, and does not examine the content or sequence of the packets. It is faster and simpler than a stateful packet inspection firewall, but also less secure and more vulnerable to attacks.

NEW QUESTION: 401
從安全營運的角度來看，下列哪一項外包協議條款具有最高優先順序？
A. 阻止使用分包商的條件
B. 發生災難時重新協商合約的條款
C. 事件期間解決問題的升級流程
D. 應用程式效能問題的根本原因分析
Answer: C (LEAVE A REPLY)
An escalation process for problem resolution during incidents is a provision that defines how to escalate and resolve issues that arise during security incidents, such as breaches, attacks, or disruptions. An escalation process is a high priority from a security operations perspective, as it can help to minimize the impact and duration of the incidents, as well as to coordinate the response and recovery efforts among the involved parties. An escalation process may include the following elements: the roles and responsibilities of the incident response team, the communication channels and methods, the criteria and thresholds for escalation, the escalation levels and procedures, the escalation matrix and contacts, and the escalation reporting and feedback.

NEW QUESTION: 402
以下哪口最能描述“可用性”作口中央情口局三要素之一的含口？
A. 确保只有授口人口才能口口信息
B. 确保信息准确无口且未被不当口改
C. 确保授口用口在需要口可以口口和使用系口和数据。
D. 确保用口采取的操作无法在事后被否口。
Answer: C (LEAVE A REPLY)

Availability ensures that information, systems, and resources are accessible and functional for authorized users whenever needed, typically achieved through redundancy, fault tolerance, backups, and disaster recovery planning, protecting against disruptions such as outages, denial- of-service attacks, or hardware failure.

NEW QUESTION: 403
下列何者最能減輕針對使用身分聯合和安全性斷言標記語言 (SAML) 所實施的系統的重播攻擊？
A. 雙重認證
B. 數位憑證和硬體令牌
C. 定時會話和安全通訊端層 (SSL)
D. 包含字母數字和特殊字元的密碼
Answer: C (LEAVE A REPLY)
The best way to mitigate a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation is to use timed sessions and Secure Socket Layer (SSL). A replay attack is a type of network attack that involves capturing and retransmitting a valid message or data to gain unauthorized access or perform malicious actions. Identity federation is a process that enables the sharing of identity information across different security domains, such as different organizations or applications. SAML is a standard protocol that enables identity federation by using XML-based assertions to exchange authentication and authorization information. To prevent a replay attack, the system can use timed sessions and SSL. Timed sessions are sessions that have a limited duration and expire after a certain period of time or inactivity. SSL is a protocol that provides encryption and authentication for data transmission over the internet. By using timed sessions and SSL, the system can ensure that the SAML assertions are valid, fresh, and secure, and that they cannot be reused or tampered with by an attacker. Two-factor authentication, digital certificates and hardware tokens, and passwords with alpha-numeric and special characters are not the best ways to mitigate a replay attack against a system using identity federation and SAML implementation, as they do not address the specific vulnerabilities of the SAML protocol or the network transmission.

NEW QUESTION: 404
哪一種報告類型要求服務組織描述其係統並定義與使用者財務報告口部控制相關的控制目標和控制措施？
A. 審計標準聲明 (SAS)70
B. 服務組織控制 1 (SOC1)
C. 服務組織控制 2 (SOC2)
D. 服務組織控制 3 (SOC3)
Answer: B (LEAVE A REPLY)
Service Organization Control 1 (SOC1) is a report that provides information about the controls at a service organization that may affect the user entities' internal control over financial reporting. It is intended for users who have a reasonable understanding of the nature and significance of the service provided, the service organization's system, and the applicable trust services criteria. A SOC 1 report

can help an organization evaluate the effectiveness of the service organization's controls that are relevant to users internal control over financial reporting.

NEW QUESTION: 405
為什麼高階管理層明確傳達正式的最大可容忍停機時間 (MTD) 決策很重要？
A. 為每位經理提供選擇適當恢復方案的精確指導
B. 向監管機構表明公司認真對待業務連續性
C. 向董事會證明高階管理層致力於連續性復原工作
D. 根據口部審計的要求提供高階管理層的正式聲明，以證明良好的商業實踐
Answer: A (LEAVE A REPLY)
The Maximum Tolerable Downtime (MTD) is the maximum period of time that a business process can be down before causing significant harm or disruption to the organization's operations.
Clearly communicating the MTD decision helps ensure that managers and recovery teams understand the time constraints they are working with and can select and implement appropriate recovery alternatives within that timeframe.
By establishing MTD, the organization ensures that:
Recovery strategies are in place for critical business functions.
Managers know the urgency and can make informed decisions about resources, personnel, and recovery processes that align with the defined MTD.

NEW QUESTION: 406
哪個軟體定義網路 (SDN) 架構元件負責轉換網路需求？
A. SDN 應用程式
B. SDN 資料路徑
C. SDN 控制器
D. SDN 北向介面
Answer: C (LEAVE A REPLY)
Software defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for more flexibility and programmability of network functions. The SDN controller is the architectural component that acts as the brain of the SDN network, communicating with both the SDN applications and the SDN data paths. The SDN controller is responsible for translating the network requirements from the SDN applications, such as security policies, routing rules, or load balancing, into instructions for the SDN data paths, such as switches, routers, or firewalls, to implement them. The SDN controller also monitors the network state and provides feedback to the SDN applications.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest**

Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 407
當使用安全性斷言標記語言 (SAML) 時，假定主體
A. 接受來自系統的持久cookie。
B. 允許使用安全通訊端層 (SSL) 進行資料交換。
C. 位於支援遠端授權的系統上。
D. 向至少一個身分提供者註冊。
Answer: D (LEAVE A REPLY)
When using Security Assertion Markup Language (SAML), it is assumed that the principal subject enrolls with at least one identity provider. The principal subject is the entity that requests access to a resource or service, such as a user, device, or application. The identity provider is the entity that authenticates and asserts the identity and attributes of the principal subject, such as a directory service, a certificate authority, or a social media platform. The principal subject must enroll with the identity provider and obtain a credential, such as a username, password, token, or certificate, that can be used to prove its identity and authorization.

NEW QUESTION: 408
下列哪一項最能描述選定的明文攻擊？
A. 密碼分析者可以從任意文字□生密文。
B. 密碼分析者檢□來回傳送的通訊。
C. 密碼分析者可以選擇金鑰和演算法來發動攻擊。
D. 提供密碼分析者密文，從中確定原始訊息
Answer: (SHOW ANSWER)
According to the CISSP CBK Official Study Guide, a chosen plaintext attack is a type of cryptanalysis that allows the cryptanalyst to generate ciphertext from arbitrary text. A cryptanalysis is the process of breaking or analyzing a cryptographic system or algorithm, by finding the plaintext, the key, or the algorithm from the ciphertext, or by exploiting the weaknesses or vulnerabilities of the system or algorithm. A chosen plaintext attack is a scenario where the cryptanalyst has access to the encryption function or device, and can choose any plaintext and obtain the corresponding ciphertext. A chosen plaintext attack can help the cryptanalyst to deduce the key or the algorithm, or to create a codebook or a dictionary that maps the plaintext to the ciphertext. The cryptanalyst does not examine the communication being sent back and forth, as this would be a ciphertext-only attack, where the cryptanalyst only has access to the ciphertext, and tries to infer the plaintext, the key, or the algorithm from the statistical or linguistic analysis of the ciphertext. The cryptanalyst does not choose the key and algorithm to mount the attack, as this would be a known plaintext attack, where the cryptanalyst has access to some pairs of plaintext and ciphertext that are encrypted with the same key and algorithm, and tries to find the key or the algorithm from the correlation or pattern between the plaintext and the ciphertext. The cryptanalyst is not presented with the ciphertext from which the original message is

determined, as this would be a decryption problem, where the cryptanalyst has access to the ciphertext and the key or the algorithm, and tries to recover the plaintext from the ciphertext.

NEW QUESTION: 409
下列哪一項是與使用基於 Web 的用口端輸入驗證相關的威脅？
A. 驗證發生後使用者將能口變更輸入
B. 網路伺服器無法在傳輸後驗證輸入
C. 客口端系統可能從網路伺服器接收到無效輸入
D. 網路伺服器將無法從客口端接收無效輸入
Answer: (SHOW ANSWER)
A threat related to the use of web-based client side input validation is that users would be able to alter the input after validation has occurred. Client side input validation is performed on the user's browser using JavaScript or other scripting languages. It can provide a faster and more user- friendly feedback to the user, but it can also be easily bypassed or manipulated by an attacker who disables JavaScript, uses a web proxy, or modifies the source code of the web page.
Therefore, client side input validation should not be relied upon as the sole or primary method of preventing malicious or malformed input from reaching the web server. Server side input validation is also necessary to ensure the security and integrity of the web application.

NEW QUESTION: 410
哪種類型的火災警報系統感測器旨在儘早偵測火災？
A. 電離
B. 紅外線
C. 熱
D. 光電
Answer: A (LEAVE A REPLY)
Ionization is a type of fire alarm system sensor that is intended to detect fire at its earliest stage. Ionization sensors use a small amount of radioactive material to ionize the air inside a chamber. When smoke enters the chamber, it disrupts the ionization process and reduces the current flow, which triggers the alarm. Ionization sensors are more sensitive to small particles of smoke, such as those produced by flaming fires, than other types of sensors, such as photoelectric or thermal sensors.

NEW QUESTION: 411
下列哪一項在偵測傳輸控制協定/網際網路協定 (TCP/IP) 流量中資訊隱藏的方面最為有效？
A. 狀態偵測防火牆
B. 應用層防火牆
C. 口容過濾代理
D. 封包過濾防火牆
Answer: B (LEAVE A REPLY)
An application-level firewall is the most effective in detecting information hiding in TCP/IP traffic.

Information hiding is a technique that conceals data or messages within other data or messages, such as using steganography, covert channels, or encryption. An application-level firewall is a type of firewall that operates at the application layer of the OSI model, and inspects the content and context of the network packets, such as the headers, payloads, or protocols. An application- level firewall can help to detect information hiding in TCP/IP traffic, as it can analyze the data for any anomalies, inconsistencies, or violations of the expected format or behavior. A stateful inspection firewall, a content-filtering proxy, and a packet-filter firewall are not as effective in detecting information hiding in TCP/IP traffic, as they operate at lower layers of the OSI model, and only inspect the state, content, or header of the network packets, respectively.

NEW QUESTION: 412
以下哪□最能描述“重放攻□”？
A. 攻□者□截并重新□□有效的数据□□，以□取未□授□的□□□限或重复交易。
B. 攻□者利用□量流量淹没目□。
C. 攻□者利用□冲区溢出漏洞
D. 攻□者使用常用□字典猜□密□
Answer: A (LEAVE A REPLY)
In a replay attack, an attacker captures legitimate data (such as an authentication token or transaction) and retransmits it later to impersonate the original sender or repeat the transaction. Countermeasures include timestamps, nonces, and sequence numbers to ensure freshness.

NEW QUESTION: 413
以下哪□最能描述“数字主□”与“数据主□”的区□？
A. 数字主□和数据主□是相同的概念。
B. 数字主□是一个更广泛的概念，涵盖一个国家或□□□其数字基□□施、技□□和数据的控制□，而数据主□□特指□存□或□理的数据的法律管□□。
C. 数字主□□适用于个人用□，不适用于□□或国家。
D. 数字主□特指知□□□。
Answer: B (LEAVE A REPLY)
Digital sovereignty is a broader concept encompassing a nation's or organization's control over its overall digital infrastructure, technology dependencies, and strategic autonomy, while data sovereignty is a more specific subset concerned particularly with the legal jurisdiction and regulatory requirements governing where data is stored and processed-both are increasingly relevant considerations in cloud strategy and geopolitical risk assessment.

NEW QUESTION: 414
公司需要向外部業務合作夥伴提供雲端儲存上敏感資料的共用存取。下列哪一種身分識別模型最適合隱藏身分識別提供者 (IdP) 和依賴方 (RP)，從不洩漏其他方的訂□清單？
A. 聯邦當局
B. 代理聯合

C. 靜態註冊
D. 動態註冊
Answer: B (LEAVE A REPLY)
Proxied federation is a type of identity federation model that is best suited for providing shared access of sensitive data on a cloud storage to external business partners, while blinding the identity providers and relying parties from each other. In proxied federation, a third-party entity, called the proxy, acts as an intermediary between the identity providers and relying parties, and handles the authentication and authorization requests and responses on their behalf. The proxy does not disclose the subscriber lists of the identity providers or relying parties to each other, and only shares the necessary attributes or claims to enable the access. The proxy also provides a single point of management, auditing, and policy enforcement for the federation.

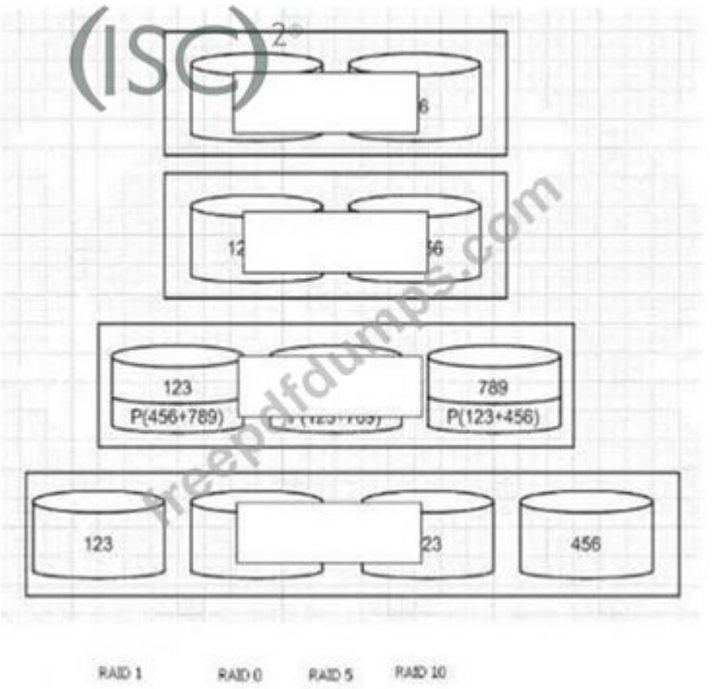
NEW QUESTION: 415
客口審口了漏洞評估報告，並指出其口容不準確。客口表示，報告中列出的漏洞無效，因為主機作業系統 (OS) 未被正確偵測。請問，漏洞評估過程中最可能出現哪個環節出現錯誤？
A. 檢測
B. 枚舉
C. 報告
D. 發現
Answer: (SHOW ANSWER)
Detection is the stage in the vulnerability assessment process where the error most likely occurred. Detection is the process of identifying the vulnerabilities that exist on the target system or network, using various tools and techniques, such as scanners, sniffers, or exploit frameworks.
Detection relies on the accurate identification of the host's operating system, as different operating systems may have different vulnerabilities. If the host's operating system was not properly detected, the detection process may produce false positives or false negatives, resulting in an inaccurate vulnerability assessment report.

NEW QUESTION: 416
初始安全分類應在系統生命週期的早期完成，並應定期進行審口。為什麼正確完成此操作很重要？
A. 決定安全要求。
B. 它影響認證和認可過程中的其他步驟。
C. 它決定功能和操作要求。
D. 系統工程流程與選定的安全控制一起運作。
Answer: A (LEAVE A REPLY)
The initial security categorization of a system plays a foundational role in defining the system's security requirements. This categorization determines the level of protection needed based on the confidentiality, integrity, and availability of the system's data and operations. The security categorization will guide the selection of appropriate security controls to mitigate risks and ensure the system meets security objectives.

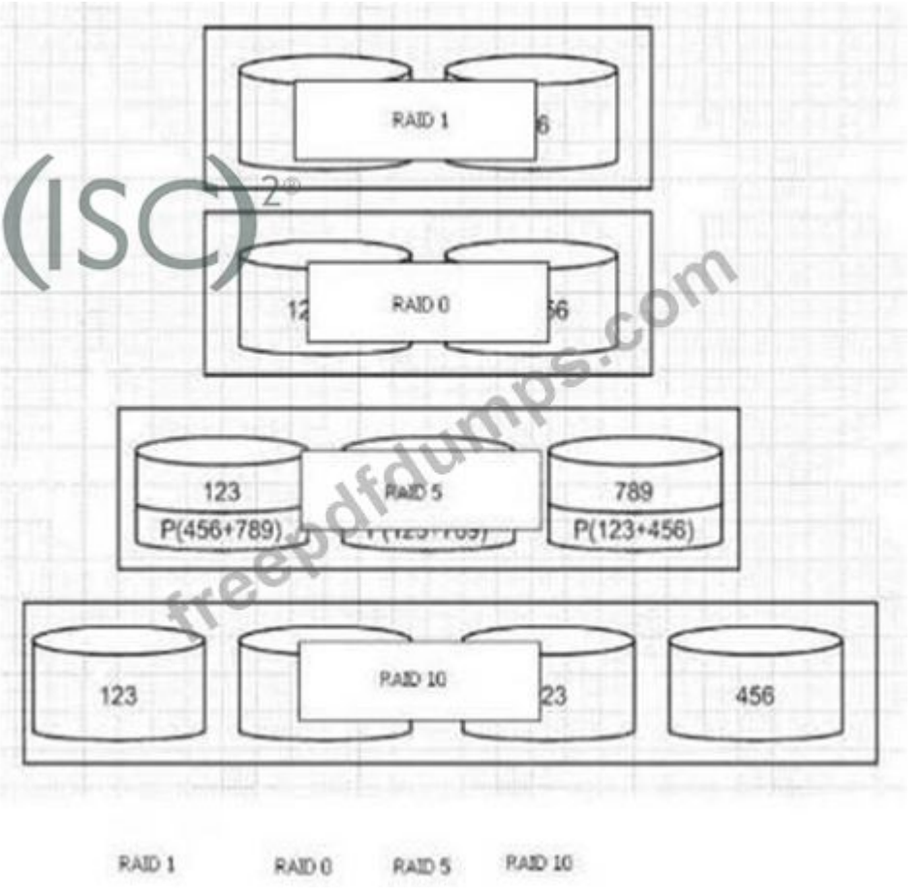
Security categorization helps establish a baseline for security controls by identifying the criticality of the system and its data, which directly influences the level of security measures required (e.g., encryption, access controls, auditing, etc.).

NEW QUESTION: 417
為什麼開放式Web應用程式安全專案(OWASP)應用程式安全驗證標準(ASVS)1級應該被視為任何Web應用程式的最低保護等級？
A. ASVS 1 等級確保應用程式不會受到 OWASP 前 10 大威脅的影響。
B. 機會主義攻擊者會尋找任何容易被利用的漏洞應用程式。
C. 大多數監管機構將 ASVS 1 等級視為應用程式的基本控制措施。
D. ASVS 1 等級應用程式安全性可為敏感資料提供充分的保護。
Answer: (SHOW ANSWER)
OWASP Application Security Verification Standards (ASVS) Level 1 is the lowest level of protection for any web application, as it only requires automated verification of the security controls. ASVS Level 1 should be considered a minimum level of protection, because opportunistic attackers will look for any easily exploitable vulnerable applications, and automated verification may not detect all the possible flaws or weaknesses. Option A, ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats, is incorrect, as ASVS Level 1 does not guarantee that the applications are immune to the most common web application security risks. Option C, most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications, is incorrect, as most regulatory bodies require higher levels of verification and assurance for applications that handle sensitive or regulated data. Option D, securing applications at ASVS Level 1 provides adequate protection for sensitive data, is incorrect, as ASVS Level 1 is not sufficient for protecting sensitive data, and higher levels of verification and encryption are needed.

NEW QUESTION: 418
拖放問題
給定一個包含有序號的文件，即123456789”，將以下每個冗餘獨立磁碟陣列(RAID) 等級與相應的視覺表示視覺表示相匹配。註 :P() = 奇偶校驗。
將每個等級拖曳到圖表上的適當位置。



Answer:



NEW QUESTION: 419

關於等價類測試，下列哪一項是正確的？

A. 它的特徵是函數中實現的程序的無狀態行為。

B. 只需考慮分割區中的一個代表口即可覆寫整個分割區。

C. 測試輸入是從給定功能規格的導出邊界中獲得的。

D. 它可用於測試通訊協定和圖形使用者介面。

Answer: B (LEAVE A REPLY)

Equivalence class testing is a software testing technique that divides the input domain of a program into a finite number of equivalence classes, or partitions, based on the expected behavior or output of the program. An equivalence class is a set of inputs that are equivalent in terms of satisfying the same condition or producing the same result. The main idea of equivalence class testing is that an entire partition can be covered by considering only one representative value from that partition, as all the values in the same partition are expected to behave the same way. This can reduce the number of test cases and increase the test coverage and efficiency.

NEW QUESTION: 420

可以透過應用下列哪一項來開發安全編碼？

A. 應用組織的可接受的使用指南

B. 應用業界最佳實踐編碼指南

C. 應用快速應用程式開發 (RAD) 編碼

D. 應用組織的 Web 應用程式防火牆 (WAF) 策略

Answer: (SHOW ANSWER)

Secure coding can be developed by applying the industry best practice coding guidelines. Secure coding is the practice of writing software that is free from vulnerabilities or defects that could compromise the security, functionality, or performance of the software or the system. Secure coding aims to prevent or mitigate the exploitation of the software by attackers, who could use the software to gain unauthorized access, execute malicious commands, steal or manipulate data, or cause denial of service. Secure coding can be developed by applying the industry best practice coding guidelines, which are sets of rules or standards that define the best practices for writing secure, reliable, and maintainable code. The industry best practice coding guidelines provide the recommendations and examples for the secure coding techniques, such as input validation, output encoding, error handling, encryption, or logging. The industry best practice coding guidelines also provide the common coding errors or vulnerabilities to avoid, such as buffer overflow, SQL injection, cross-site scripting, or insecure cryptography. Some examples of the industry best practice coding guidelines are the OWASP Secure Coding Practices, the CERT Secure Coding Standards, or the ISO/IEC 27034 Application Security.

NEW QUESTION: 421

為了防止智慧型手機受到惡意軟體攻擊，下列哪一項措施是最關鍵的？

A. 口用強密碼。

B. 安裝行動防毒軟體。

C. 口用生物辨識身份驗證。

D. 防止越獄或生根。

Answer: (SHOW ANSWER)

The most critical measure in order to safeguard from a malware attack on a smartphone is to prevent jailbreaking or rooting. Jailbreaking or rooting is the process of removing the manufacturer's or carrier's

restrictions on a smartphone, which allows the user to install unauthorized apps or modify the system settings. However, this also removes a lot of the built-in security features of the smartphone, such as encryption, sandboxing, and app verification, and exposes the device to malware infections and attacks. Therefore, it is advisable to avoid jailbreaking or rooting your smartphone and to download apps only from reputable sources.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 422
以下哪□最能描述“内部威□：非故意疏忽)内部人□”与“故意(疏忽)内部人□”之□的关系？
“□意内鬼”？
A. □两个□□描述的是同一种威□行□者和行□。
B. 疏忽的内部人□因粗心、□□或缺乏意□而造成□害，并非出于□意；而□意的内部人□□故意□求造成□害，例如通□数据窃取或破坏等方式。
C. 疏忽的内部人□只能是外部承包商，□不可能是全□□工。
D. □意内部人□的□机始□□限于□□利益。
Answer: B (LEAVE A REPLY)
A negligent (unintentional) insider causes harm to the organization through carelessness, human error, or a genuine lack of security awareness-such as accidentally emailing sensitive data to the wrong recipient-without any malicious intent. A malicious insider, by contrast, intentionally seeks to cause harm, such as through deliberate data theft, sabotage, or fraud, often motivated by financial gain, grievance, or ideology, requiring different detection and mitigation approaches for each threat type.

NEW QUESTION: 423
下列哪一項是避免磁介質資料剩磁的有效方法？
A. 消磁
B. 加密
C. 資料遺失防護 (DLP)
D. 身份驗證
Answer: (SHOW ANSWER)
Degaussing is an effective method for avoiding magnetic media data remanence, which is the residual representation of data that remains on a storage device after it has been erased or overwritten.
Degaussing is a process of applying a strong magnetic field to the storage device, such as a hard disk or a tape, to erase the data and destroy the magnetic alignment of the media.
Degaussing can ensure that the data is unrecoverable, even by forensic tools or techniques.

Encryption, DLP, and authentication are not methods for avoiding magnetic media data remanence, as they do not erase the data from the storage device, but rather protect it from unauthorized access or disclosure.

NEW QUESTION: 424
僅依靠軟體能力成熟度模型 (CMM) 來指導流程改善和評估所購買軟體的能力，下列哪一項是最大的風險？
A. 組織在使用 CMM 時只能達到成熟度等級 3
B. CMM 沒有明確解決安全問題
C. 座標測量機只能用於□部開發的軟體
D. CMM 是特定於供應商的並且可能存在偏差
Answer: B (LEAVE A REPLY)
The greatest risk of relying only on Capability Maturity Models (CMMs) for software to guide process improvement and assess capabilities of acquired software is that CMMs do not explicitly address safety and security. CMMs are frameworks that measure and improve the maturity and quality of the software development processes and products. CMMs define different levels of maturity, from initial to optimized, based on the presence and effectiveness of the key process areas, such as requirements management, project planning, configuration management, quality assurance, or risk management. CMMs can help to evaluate and improve the software development processes and products, but they do not explicitly address the safety and security aspects of the software. Safety and security are important attributes of the software, especially for critical or sensitive applications, such as medical, military, or financial applications. Safety and security require specific processes and practices, such as threat modeling, secure coding, vulnerability testing, or incident response, that are not covered by the CMMs. Therefore, relying only on CMMs for software may result in overlooking or neglecting the safety and security issues of the software, which may lead to serious consequences, such as harm, loss, or breach.
Organizations can only reach a maturity level 3 when using CMMs, CMMs can only be used for software developed in-house, and CMMs are vendor specific and may be biased are not the greatest risks of relying only on CMMs for software. These are some of the limitations or challenges of using CMMs for software, but they are not as significant or critical as the lack of safety and security.
Organizations can reach higher maturity levels than level 3 when using CMMs, depending on the implementation and assessment of the CMMs. CMMs can be used for software developed in-house or outsourced, depending on the scope and criteria of the CMMs.
CMMs are not vendor specific and may not be biased, as they are based on industry standards and best practices, such as ISO/IEC 15504 or ISO/IEC 33001.

NEW QUESTION: 425
以下哪□最能描述“出口□□限制”作□一种安全相关控制措施的目的？
A. 自□加密出站数据
B. 限制出站数据□□速率，即使其他控制措施失效，也能帮助减□或限制大□模数据泄露的影响
C. □了提高入站网□性能

D. 消除口DLP解决方案的需求

Answer: (SHOW ANSWER)

Egress bandwidth throttling limits the rate at which data can be transferred out of a network, which-while not a primary detection or prevention control-can act as a supplementary safeguard by slowing the speed at which large volumes of data could be exfiltrated, potentially providing more time for detection and response before significant data loss occurs.

NEW QUESTION: 426

應在下列哪個系統生命週期過程中製定安全要求？

A. 風險管理

B. 商業分析

C. 資訊管理

D. 系統分析

Answer: D (LEAVE A REPLY)

Security requirements should be developed in the system analysis process of the system life cycle. System life cycle is the process of creating or modifying a system, from the initial conception to the final disposal. System life cycle follows a model, such as waterfall, agile, or spiral, that defines the phases and activities of the system development process. System analysis is one of the phases of the system life cycle, where the current system is studied and the needs and expectations of the users and stakeholders are identified and defined. System analysis also involves the development of the security requirements, which are the statements that specify the security objectives, functions, and constraints of the system. Security requirements should be developed in the system analysis process, because:
It can ensure that the security is integrated and embedded in the system design and implementation, rather than added or patched as an afterthought.
It can reduce the cost and complexity of the system development, as the security issues and defects can be detected and fixed early in the system development process, rather than later when they are more expensive and difficult to resolve.
It can improve the quality and effectiveness of the system, as the security requirements can ensure that the system meets the security standards and best practices, and satisfies the security needs and expectations of the users and stakeholders.

NEW QUESTION: 427

在處理網路犯罪時，刑法難以執行的主要原因是什麼？

A. 引渡條約很少被執行。

B. 存在許多語言障礙。

C. 執法機關人手不足。

D. 管轄權難以界定。

Answer: D (LEAVE A REPLY)

Jurisdiction is the authority and power of a legal entity, such as a state or a court, to enforce laws and regulations within a specific territory or domain. Jurisdiction is hard to define when dealing with cybercrime, as cybercrime can transcend physical and geographical boundaries, and involve multiple

actors, victims, and locations. The primary reason criminal law is difficult to enforce when dealing with cybercrime is that different jurisdictions may have different laws, definitions, standards, and procedures for cybercrime, and may not cooperate or coordinate with each other.
Extradition treaties are agreements between states that allow the transfer of a person who is accused or convicted of a crime from one state to another. Extradition treaties may not be enforced due to political, diplomatic, or human rights reasons, but this is not the primary reason for the difficulty of enforcing criminal law for cybercrime. Language barriers may exist between different jurisdictions, but they can be overcome with translation and interpretation services. Law enforcement agencies may be understaffed or under-resourced to deal with cybercrime, but this is not the primary reason for the difficulty of enforcing criminal law for cybercrime.

NEW QUESTION: 428
以下哪□最能描述“哈希□□攻□”？
A. 攻□者使用暴力破解技□破解密□哈希□，从而恢复明文密□
B. 攻□者捕□哈希凭□，并直接使用□凭□□系□□行身份□□，而无需知道或破解底□明文密□。
C. 攻□者向□□服□器□送大量登□□求，□致□□服□器崩□。
D. 攻□者利用哈希算法数学□构中的漏洞。
Answer: B (LEAVE A REPLY)
In a pass-the-hash attack, an adversary captures a hashed credential (such as an NTLM hash) from a compromised system's memory and uses it directly to authenticate to other systems that accept the hash as a valid credential, without ever needing to crack or know the underlying plaintext password, exploiting how certain authentication protocols validate hashed credentials.

NEW QUESTION: 429
實施企業級業務連續性計畫需要下列哪些條件？
A. 組織□部溝通良好
B. 災難復原(DP)專案團隊的組建
C. 已完成的業務影響分析 (BIA)
D. 有據可□的資訊資□分類
Answer: A (LEAVE A REPLY)
The adoption of an enterprise-wide business continuity program requires good communication throughout the organization. A business continuity program is a set of policies, procedures, and plans that aim to ensure the continuity of critical business functions and processes in the event of a disruption or disaster. Good communication throughout the organization is essential for the adoption of a business continuity program, because it helps to raise awareness, gain support, coordinate activities, and share information among the stakeholders involved in the business continuity process. Formation of a disaster recovery project team, a completed business impact analysis, and well- documented information asset classification are not the requirements for the adoption of an enterprise-wide business continuity program, although they are important components of the business continuity process. A disaster recovery project team is a group of people who are responsible for planning, implementing, and testing the disaster recovery strategies and procedures for a specific business unit

or function. A business impact analysis is a process of identifying and evaluating the potential impacts of a disruption or disaster on the business objectives, functions, and processes. An information asset classification is a process of assigning labels or categories to the information assets based on their value, sensitivity, and criticality to the organization.

NEW QUESTION: 430
開放系統互連 (OSI) 參考模型中哪一層處理資料包分段與重組？
A. 會話
B. 運輸
C. 資料鏈路
D. 網絡
Answer: D (LEAVE A REPLY)
The layer that handles packet fragmentation and reassembly in the Open System Interconnection (OSI) reference model is the network layer. The network layer is the third layer of the OSI model, and it is responsible for routing and forwarding packets across different networks. The network layer also performs packet fragmentation and reassembly, which are processes that divide a large packet into smaller fragments to fit the maximum transmission unit (MTU) of the underlying network, and reassemble the fragments back into the original packet at the destination. Packet fragmentation and reassembly can improve the efficiency and reliability of data transmission, as well as avoid congestion and errors.

NEW QUESTION: 431
什麼測試技術使設計人員能□針對潛在漏洞制定緩解策略？
A. 手動檢□與審核
B. 滲透測試
C. 威脅建模
D. 原始碼審□
Answer: C (LEAVE A REPLY)
Threat modeling is the testing technique that enables the designer to develop mitigation strategies for potential vulnerabilities. Threat modeling is a method of identifying, analyzing, and prioritizing the threats and vulnerabilities that may affect a system or an application. Threat modeling can help the designer to understand the attack surface, the attack vectors, the attack scenarios, and the impact and likelihood of the attacks. Threat modeling can also help the designer to develop mitigation strategies for the potential vulnerabilities, such as applying security controls, implementing security best practices, or redesigning the system or the application.
Threat modeling can be performed at any stage of the system development life cycle (SDLC), but it is most effective when done early and iteratively.

NEW QUESTION: 432
下列哪一項是處理突發事件的基本目標？
A. 恢復對受影響系統的控制

B. 沒收嫌疑犯的電腦
C. 起訴攻擊者
D. 執行系統完整備份
Answer: (SHOW ANSWER)
A fundamental objective in handling an incident is to restore control of the affected systems as soon as possible. An incident is an event or a situation that violates or threatens the security, confidentiality, integrity, or availability of an organization's information assets or resources.
Handling an incident is the process of responding to, containing, analyzing, recovering from, and reporting on an incident, with the aim of minimizing the impact and preventing the recurrence of the incident. Restoring control of the affected systems is a crucial objective in handling an incident, as it can help to resume the normal operations, services, and functions of the organization, and to mitigate the damage or loss caused by the incident. Confiscating the suspect's computers, prosecuting the attacker, and performing full backups of the system are not fundamental objectives in handling an incident, as they are more related to the investigation, legal, or recovery aspects of the incident, which may not be as urgent or essential as restoring control of the affected systems.

NEW QUESTION: 433
使用 OAuth(開放授權標準)2.0 為服務整合第三方身分提供者時，下列哪一個問題無法解決？
A. 資源伺服器需要使用密碼來驗證最終使用者身分。
B. 撤銷第三方部分使用者的存取權限，而不是撤銷第三方所有使用者的存取權限
C. 第三方受到威脅意味著服務中的所有使用者都受到威脅。
D. 訪客使用者需要透過第三方身分提供者進行身分驗證。
Answer: A (LEAVE A REPLY)
The problem that is not addressed by using OAuth 2.0 to integrate a third-party identity provider for a service is that resource servers are required to use passwords to authenticate end users.
OAuth 2.0 is a framework that enables a third-party application to obtain limited access to a protected resource on behalf of a resource owner, without exposing the resource owner's credentials to the third-party application. OAuth 2.0 relies on an authorization server that acts as an identity provider and issues access tokens to the third-party application, based on the resource owner's consent and the scope of the access request. OAuth 2.0 does not address the authentication of the resource owner or the end user by the resource server, which is the server that hosts the protected resource. The resource server may still require the resource owner or the end user to use passwords or other methods to authenticate themselves, before granting access to the protected resource. Revocation of access of some users of the third party instead of all the users from the third party, compromise of the third party means compromise of all the users in the service, and guest users need to authenticate with the third party identity provider are problems that are addressed by using OAuth 2.0 to integrate a third-party identity provider for a service, as they are related to the delegation, revocation, or granularity of the access control or the identity management.

NEW QUESTION: 434
以下哪□最能描述“深度□造”技□作□一种新□安全威□？

A. 一种□□用于提高□□□□率的技□
B. 人工智能生成的合成媒体(音□、□□或□像)，能□逼真地模仿真人，可用于□施欺□散布虚假信息或□行社会工程攻□，例如冒充高管。
C. 一种□□会□通□加密方法
D. 一种用于□□□□文件中□意□件的工具
Answer: (SHOW ANSWER)
Deepfake technology uses artificial intelligence, particularly generative models, to create highly realistic but fabricated audio, video, or image content that convincingly impersonates a real individual's voice or appearance, posing an emerging security threat when used to facilitate fraud (such as convincing a finance employee to authorize a payment via a fake video call), disinformation campaigns, or enhanced social engineering attacks.

NEW QUESTION: 435
下列哪一項是最安全的密碼技術？
A. 密碼
B. 一次密碼
C. 認知密碼
D. dphertext
Answer: (SHOW ANSWER)
The most secure password technique is the one-time password. A one-time password is a password that is valid for only one login session or transaction, and that is randomly generated or derived from a secret key or algorithm. A one-time password can help to enhance the security of the authentication process, by preventing the password from being reused, guessed, stolen, or intercepted by unauthorized parties. A one-time password can also help to protect against various password-based attacks, such as replay, brute force, or phishing attacks. A one-time password can be implemented by using various methods or techniques, such as hardware tokens, software tokens, SMS messages, or biometric factors. Passphrase, cognitive password, or ciphertext are not the most secure password techniques, as they are either less complex, less random, or less dynamic than the one-time password.

NEW QUESTION: 436
以下哪□最能描述“安全意□培□”的目的？
A. □□培□IT人□如何配置防火□
B. □所有□工□行安全政策、威□及其在保□□□□□方面个人□任的教育。
C. □□工□行渗透□□人□□格□□
D. 取代技□安全控制的需求
Answer: (SHOW ANSWER)
Security awareness training educates all employees-not just IT or security staff-about organizational security policies, common threats (such as phishing and social engineering), and their individual responsibilities in protecting organizational information and assets, addressing the human element of security as a complement to technical and administrative controls.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 437
獨立磁碟冗餘陣列 (RAID) 的哪個層級配置主要用於高效能資料讀寫？
A. RAID-0
B. RAID-1
C. RAID-5
D. RAID-6
Answer: (SHOW ANSWER)
RAID-0 is the level of Redundant Array of Independent Disks (RAID) that is configured primarily for high-performance data reads and writes. RAID is a technology that combines multiple physical disks into a logical unit, and that distributes the data across the disks using different methods, such as striping, mirroring, or parity. RAID can provide benefits such as increased storage capacity, improved performance, or enhanced reliability, depending on the level of RAID that is used. RAID-0 is the level of RAID that uses striping as the method of data distribution, and that splits the data into equal-sized blocks and writes them sequentially across the disks. RAID-0 can provide benefits such as:
High-performance data reads and writes, as the data can be accessed or stored simultaneously from or to multiple disks, and as the data transfer rate is increased by the number of disks in the array.
Full utilization of the storage capacity, as the data is evenly distributed across the disks, and as there is no overhead or redundancy of the data. However, RAID-0 also has drawbacks such as:
No fault tolerance or data protection, as the failure of any disk in the array will result in the loss of the entire data, and as there is no backup or recovery of the data.
Increased risk of data corruption or inconsistency, as the data blocks may not be aligned or synchronized across the disks, and as there may be errors or delays in the data transmission or processing.

NEW QUESTION: 438
在調□某組織網站資料庫被盜事件時，儘管客□端□本進行了輸入驗證，但仍發現攻擊者使用了結構化□詢語言 (SQL) 注入技術。下列哪一項措施能最大程度地防止此類攻擊再次發生？
A. 加密伺服器之間的通信
B. 加密 Web 伺服器流量
C. 實現伺服器端過濾
D. 在邊界防火牆過濾出站流量
Answer: C (LEAVE A REPLY)

The action that provides the greatest protection against the same attack occurring again is to implement server-side filtering. Server-side filtering is the process of validating and sanitizing the user input on the server side, before passing it to the database or application. Server-side filtering can prevent SQL injection attacks, which are the attacks that exploit the vulnerability of the database or application to execute malicious SQL commands or queries. SQL injection attacks can result in data theft, corruption, or deletion, as well as unauthorized access or privilege escalation.

NEW QUESTION: 439
下列哪一個實體最終應對雲端服務供應商複製的資料中的資料殘留漏洞負責？
A. 資料擁有者
B. 資料管理員
C. 資料保管人
D. 資料處理器
Answer: A (LEAVE A REPLY)
The entity that is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider is the data owner. A data owner is a person or an entity that has the authority or the responsibility for the data or the information within an organization, and that determines or defines the classification, the usage, the protection, or the retention of the data or the information. A data owner has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization, as the data owner is ultimately accountable or liable for the security or the quality of the data or the information, regardless of who processes or handles the data or the information. A data owner can ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization, by performing the tasks or the functions such as conducting due diligence, establishing service level agreements, defining security requirements, monitoring performance, or auditing compliance.

NEW QUESTION: 440
下列何者最能代表縱深防禦概念？
A. 基於網路的資料遺失防護 (DLP)、網路存取控制 (NAC)、基於網路的入侵防禦系統 (NIPS)、核心交換器上的連接埠安全
B. 基於主機的資料遺失防護 (DLP)、端點反惡意軟體解決方案、基於主機的完整性檢口器、筆記型電腦鎖定、硬碟 (HDD) 加密
C. 端點安全管理、網路入侵偵測系統 (NIDS)、網路存取控制 (NAC)、特權存取管理 (PAM)、安全資訊與事件管理 (SIEM)
D. Web 應用程式防火牆 (WAF)、閘道網路設備調整、資料庫防火牆、新世代防火牆 (NGFW)、二級非軍事區 (DMZ) 調整
Answer: C (LEAVE A REPLY)
Defense in depth is a concept that involves implementing multiple layers of security controls to protect the assets and information of an organization. The idea is to create a series of obstacles that would

deter or delay an attacker from reaching the target, and to provide detection and response capabilities to mitigate the impact of an attack. Defense in depth can be applied at different levels, such as physical, network, host, application, data, and user. The answer choice C represents a defense in depth concept, because it includes security controls at different levels, such as endpoint security management (host level), network intrusion detection system (network level), Network Access Control (network level), Privileged Access Management (user level), and security information and event management (data level). The other answer choices are not examples of defense in depth, because they only focus on one or two levels of security, and do not provide a comprehensive protection for the organization.

NEW QUESTION: 441
攻擊者如何利用溢位來執行任意程式碼？
A. 修改函數的回傳位址。
B. 更改堆疊位址。
C. 取代堆疊中的元素。
D. 移動堆疊指標。
Answer: A (LEAVE A REPLY)
An attacker can exploit a buffer overflow to execute arbitrary code by modifying a function's return address. A buffer overflow is a condition that occurs when a program attempts to write more data to a fixed-length memory space, or buffer, than it can hold. A buffer overflow can corrupt the adjacent memory locations, which may contain important data or instructions for the program. A function's return address is the memory location that stores the address of the instruction that the program should return to after executing the function. An attacker can overwrite the return address with the address of a malicious code, which can be injected into the buffer or another location, and redirect the program flow to execute the malicious code.

NEW QUESTION: 442
實施資料使用控制的主要好處是什麼？
A. 如果資料遺失，則必須對其進行解密才能開口。
B. 如果資料遺失，未經授權的使用者將無法存取。
C. 口看資料時，只有授權使用者才能列印。
D. 口看資料時，必須使用安全協定進行存取。
Answer: B (LEAVE A REPLY)
Data-in-use controls are security measures that protect data while it is being processed or manipulated by an application or a user. Examples of data-in-use controls include encryption, masking, tokenization, and digital rights management. The primary benefit of implementing data- in- use controls is that they prevent unauthorized access to sensitive data in the event of data loss, theft, or leakage. If the data is lost, it will not be accessible to unauthorized users because it will be encrypted, masked, tokenized, or protected by digital rights.

NEW QUESTION: 443
下列哪一項是促進安全軟體開發的最佳技術？
A. 遵守正在開發的軟體應用程式的安全編碼實踐。
B. 對正在開發的軟體應用程式進行滲透測試。
C. 針對正在開發的軟體應用程式進行威脅建模審□。
D. 對正在開發的軟體應用程式執行程式碼審□程序。
Answer: A (LEAVE A REPLY)
Secure software development is a process of designing, developing, testing, and maintaining software systems or applications that meet the security requirements and standards of the organization and the stakeholders. The best technique to facilitate secure software development is to adhere to secure coding practices for the software application under development. Secure coding practices are guidelines or principles that help to prevent or mitigate common security vulnerabilities or flaws in the software code, such as buffer overflow, injection, cross-site scripting, or broken authentication. Secure coding practices can help to improve the quality, reliability, and security of the software application, as well as reduce the cost and time of fixing the security issues later. Conducting penetration testing, developing a threat modeling review, or performing a code review process are also good techniques to facilitate secure software development, but they are not as effective or proactive as adhering to secure coding practices.

NEW QUESTION: 444
以下哪□最能描述“出口点机密容器□像(已□名和□□)”的用途？
A. 加密容器□排平台的管理接口
B. □容器□像□行加密□名，并生成关于其构建来源和完整性的□明，使下游系□能□□□□部署来自已知合法来源的受信任、未修改的□像。
C. 一种□□容器□像以降低□像□□存□成本的方法
D. 一种□□用于管理容器网□策略的技□
Answer: B (LEAVE A REPLY)
Signing container images and generating build provenance attestations allows downstream deployment systems to cryptographically verify that a container image originated from a trusted, legitimate build process and has not been tampered with since it was built, helping to prevent the deployment of unauthorized, maliciously modified, or unverified images within a software supply chain.

NEW QUESTION: 445
為了量化安全計畫對組織管理的價□，安全專業人員必須執行下列哪項操作？
A. 使用指標進行報告。
B. 將優先權排列為高、中或低。
C. 傳達合規性障礙。
D. 報告員工活動
Answer: A (LEAVE A REPLY)

Reporting using metrics is the most important thing that a security professional must do in order to quantify the value of a security program to organization management. Metrics are measurable indicators that can be used to evaluate the performance, effectiveness, efficiency, and progress of a security program. Metrics can help the security professional to demonstrate the benefits, costs, risks, and return on investment of the security program, as well as to identify the gaps, weaknesses, and improvement opportunities. Metrics can also help the organization management to understand the security posture, align the security goals with the business objectives, and make informed decisions.

NEW QUESTION: 446
在編寫安全評估程序時，測試輸出和報告的主要目的是什麼？
A. 強制軟體失敗並記錄流程
B. 尋找機密性和完整性上的妥協領域
C. 允許客觀的通過或失敗決策
D. 辨識測試結果中的惡意軟體或隱藏程式碼
Answer: (SHOW ANSWER)
According to the CISSP Official (ISC)2 Practice Tests, the main purpose of the test outputs and reports when writing security assessment procedures is to find areas of compromise in confidentiality and integrity. Security assessment is the process of evaluating the security posture and effectiveness of a system, network, or application, by identifying and measuring the vulnerabilities, threats, and risks that may affect its security objectives. Security assessment procedures are the steps and methods that define how the security assessment will be conducted, such as the scope, the tools, the techniques, the criteria, and the deliverables. The test outputs and reports are the results and documentation of the security assessment, which provide the evidence and analysis of the security issues and findings. The main purpose of the test outputs and reports is to find areas of compromise in confidentiality and integrity, which are two of the core security principles that aim to protect the data and the system from unauthorized access, disclosure, modification, or destruction. The test outputs and reports may also help to find areas of compromise in availability, accountability, authenticity, or non-repudiation, which are other security principles that may be relevant for the system under assessment. The test outputs and reports are not meant to force the software to fail and document the process, although this may be a side effect of some security testing techniques, such as penetration testing or fuzz testing. The test outputs and reports are not meant to allow for objective pass or fail decisions, although they may provide some recommendations or suggestions for improving the security posture and mitigating the risks. The test outputs and reports are not meant to identify malware or hidden code within the test results, although they may detect some signs or indicators of malicious or unauthorized activities or components.

NEW QUESTION: 447
安全工程師需要將安全性整合到由小組測試實施的軟體專案中，快速 持續、獨立地開發、測試並將程式碼部署到雲端。工程師最有可能與哪個軟體開發流程整合？
A. 服務導向的架構 (SOA)
B. 螺旋方法論

C. 結構化瀑布式程式設計開發
D. DevOps 整合口品團隊 (IPT)
Answer: (SHOW ANSWER)
Devops Integrated Product Team (IPT) is a software development process that integrates development, testing, and deployment into a continuous and collaborative cycle, using agile methodologies, automation tools, and cloud services. A security engineer who is required to integrate security into a software project that is implemented by small groups that quickly, continuously, and independently develop, test, and deploy code to the cloud will most likely integrate with the Devops IPT process. This process can enable the security engineer to embed security practices and controls into each stage of the software development life cycle, such as code analysis, vulnerability scanning, configuration management, and incident response.

NEW QUESTION: 448
安全專業人員確定從先前合併繼承的許多外包合約不符合當前的安全要求。下列哪一項最能最大限度地降低這種情況再次發生的風險？
A. 合併後立即定義附加安全控制
B. 在合併團隊中納入一位採購官員
C. 合併發生前先驗證所有合約
D. 指派合規官審口合併條件
Answer: (SHOW ANSWER)
The best approach to minimize the risk of security gaps in outsourcing contracts following a merger is to verify all contracts before the merger takes place. This ensures that any existing contracts are reviewed and aligned with the current organization's security requirements, policies, and standards before the merger is finalized.
By performing a thorough review of all contracts (including outsourcing and third-party agreements), potential security issues can be identified and addressed ahead of time, rather than discovering them after the merger. This proactive measure helps ensure that security requirements are fully integrated into the new agreements, reducing the risk of non-compliance or overlooked vulnerabilities.

NEW QUESTION: 449
在下列哪種情況下，鎖定伺服器機櫃並限制對鑰匙的存取比鎖定伺服器機房以防止未經授權的存取更好？
A. 伺服器機櫃位於非共用工作區。
B. 伺服器機櫃位於隔離的伺服器集區。
C. 伺服器硬體位於偏遠地區。
D. 伺服器機櫃與多個項目共用工作空間。
Answer: (SHOW ANSWER)
In this scenario, server cabinets are located in a shared workspace where multiple teams or projects are working. Locking individual server cabinets and limiting access to keys is a better option because: Access Control: If the server room itself is locked, it may prevent legitimate users (e.g., developers, administrators) from accessing their specific servers. But, by locking only the cabinets and limiting

access to the keys, you allow different users to access their respective hardware without granting them entry to the entire server room.
Separation of Access: This method allows for more granular control of who has access to what, which is important in environments where different groups or projects are using the same physical space but need to maintain separate access to their equipment.

NEW QUESTION: 450
使用 Internet 協定安全性 (IPSec) 進行遠端存取會話時，此連線使用哪個開放系統互連(OSI) 模型層？
A. 運輸
B. 網絡
C. 數據鏈接
D. 演示
Answer: B (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a protocol that provides secure and encrypted communication between two systems or networks over the internet. IPSec operates at the network layer of the Open Systems Interconnection (OSI) model, which is the third layer that is responsible for the routing and forwarding of the network packets, such as IP, ICMP, or ARP.
IPSec uses two main protocols to secure the network communication: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data integrity and authentication for the IP packets, while ESP provides data confidentiality, integrity, and authentication for the IP packets. IPSec also uses two main modes to secure the network communication: transport mode and tunnel mode. Transport mode encrypts only the payload of the IP packet, while tunnel mode encrypts both the header and the payload of the IP packet. Transport, data link, or presentation are not the OSI model layers that IPSec uses. Transport is the fourth layer that is responsible for the reliable and error-free delivery of the data segments, such as TCP, UDP, or SCTP. Data link is the second layer that is responsible for the transmission and reception of the data frames, such as Ethernet, Wi-Fi, or PPP. Presentation is the sixth layer that is responsible for the formatting and conversion of the data, such as ASCII, JPEG, or SSL.

NEW QUESTION: 451
下列何者最能描述邊界網關協定 (BGP) 的用途？
A. 維護網際網路路由器之間的網路路徑清單。
B. 向相鄰第 3 層設備提供路由資訊協定 (RIP) 版本 2 通告。
C. 為支援雲端的應用程式提供防火牆服務。
D. 維護自治系統之間有效網路路徑的清單。
Answer: D (LEAVE A REPLY)
The best description of the purpose of Border Gateway Protocol (BGP) is that it maintains a list of efficient network paths between autonomous systems. BGP is a type of routing protocol that is used to exchange routing and reachability information among different networks or autonomous systems on the internet. An autonomous system is a collection of networks or routers that are under the same

administrative control or authority, and that share a common routing policy. BGP maintains a list of efficient network paths between autonomous systems, by selecting the best routes based on various factors, such as the number of hops, the bandwidth, the latency, or the policy preferences. BGP can improve the performance, reliability, and security of the internet, and support the scalability and diversity of the internet topology.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 452
下列哪一項會影響資料的分類？
A. 指派的安全標籤
B. 多層安全性 (MLS) 架構
C. 最小口詢大小
D. 時間的流逝
Answer: D (LEAVE A REPLY)
The passage of time is one of the factors that affects the classification of data. Data classification is the process of assigning a level of sensitivity or criticality to data based on its value, impact, and legal requirements. Data classification helps to determine the appropriate security controls and handling procedures for the data. However, data classification is not static, but dynamic, meaning that it can change over time depending on various factors. One of these factors is the passage of time, which can affect the relevance, usefulness, or sensitivity of the data. For example, data that is classified as confidential or secret at one point in time may become obsolete, outdated, or declassified at a later point in time, and thus require a lower level of protection. Conversely, data that is classified as public or unclassified at one point in time may become more valuable, sensitive, or regulated at a later point in time, and thus require a higher level of protection. Therefore, data classification should be reviewed and updated periodically to reflect the changes in the data over time.

NEW QUESTION: 453
在容錯系統中，回滾功能允許什麼？
A. 將系統恢復到先前的功能狀態
B. 辨識導致問題的錯誤
C. 允許系統以簡化的方式
D. 隔離導致問題的錯誤
Answer: A (LEAVE A REPLY)

Fault-tolerant systems are systems that can continue to operate despite the occurrence of faults, errors, or failures in some of their components. Fault-tolerant systems use redundancy, diversity, and error detection and correction mechanisms to achieve high availability, reliability, and resilience. Rollback capabilities are one of the mechanisms that enable fault tolerance, which allow the system to restore itself to a previous functional state before the fault occurred. Rollback capabilities can be implemented using checkpoints, snapshots, backups, or logs that record the state of the system at regular intervals or before critical operations. If a fault is detected, the system can revert to the most recent or closest checkpoint, snapshot, backup, or log that represents a valid and consistent state of the system, and resume its normal operation from there.

NEW QUESTION: 454
哪種技術是在聯合身份解決方案中填充基於雲端的目錄的先決條件？
A. 通知工具
B. 訊息佇列工具
C. 安全性令牌工具
D. 同步工具
Answer: (SHOW ANSWER)
A federated identity solution is a system that allows users to access multiple applications and domains using a single set of credentials. A cloud-based directory is a centralized repository of user identities and attributes that can be accessed by different service providers over the internet.
A synchronization tool is a technology that enables the transfer and update of user data between the cloud-based directory and the local or on-premises directory. A synchronization tool is a prerequisite for populating the cloud-based directory in a federated identity solution, as it ensures that the user information is consistent and accurate across the federated domains.

NEW QUESTION: 455
在 Internet 協定語音 (VoIP) 網路中設定可擴充身份驗證協定 (EAP) 時，下列哪一種驗證類型最安全？
A. EAP-傳輸層安全 (TLS)
B. 透過安全隧道進行 EAP 彈性驗證
C. EAP 隧道傳輸層安全性 (TLS)
D. EAP 保護的可擴充驗證協定 (PEAP)
Answer: A (LEAVE A REPLY)
The most secure authentication type for configuring EAP in a VoIP network is EAP-Transport Layer Security (TLS). EAP is a type of framework that provides a mechanism for authenticating and authorizing the users or the devices that access a network or a service, using various methods, such as passwords, certificates, tokens, or biometrics. EAP can support various types of networks or services, such as wireless, wired, or VoIP. VoIP is a type of technology that allows the transmission and delivery of voice communications and multimedia sessions over the internet or a network, using various protocols, such as Session Initiation Protocol (SIP) or Real-time Transport Protocol (RTP). VoIP can provide various benefits, such as reducing the communication cost or complexity, and enhancing the communication quality or functionality.

EAP-TLS is a type of EAP method that uses Transport Layer Security (TLS) to provide a secure and mutual authentication and encryption for the users or the devices that access a network or a service, using certificates. EAP-TLS can provide various benefits, such as preventing or mitigating the attacks, such as man-in-the-middle, replay, or brute force, and ensuring the confidentiality, integrity, or availability of the communication or the data. EAP-TLS is the most secure authentication type for configuring EAP in a VoIP network, as it can protect the VoIP network or service from potential threats, such as eavesdropping, interception, modification, or denial of service.

NEW QUESTION: 456
下列哪一種組合對可用性的負面影響最大？
A. 拒□服務 (DoS) 攻擊和過時的硬體
B. 未經授權的交易和過時的硬件
C. 火災和數據意外更改
D. 未經授權的交易和拒□服務攻擊
Answer: (SHOW ANSWER)
Availability refers to ensuring that services, systems, and data are accessible when needed. The most critical threats to availability typically involve disruptions to access or performance.
Denial of Service (DoS) attacks are designed specifically to overwhelm a system, causing it to become unavailable. These attacks can render services or systems inaccessible by flooding them with traffic or exploiting vulnerabilities, thereby disrupting availability.
Outdated hardware can also negatively affect availability, as older hardware is more likely to fail or experience performance bottlenecks. This can lead to system outages, slower performance, and increased maintenance needs, all of which compromise availability.
Together, these two factors-DoS attacks and outdated hardware-combine to create a significant risk to availability, making A the most impactful combination.

NEW QUESTION: 457
以下哪□最能描述“□□□□性：恢复□序?
A. 同□恢复所有系□，不考□□先□。
B. 根据□□影响分析 (BIA) 确定的关□性，□先□定一个□先□□序，用于在中断后恢复系□和□□功能，确保在可用□源限制内首先恢复最关□的功能。
C. 按照系□故障的完全相反□序□行恢复
D. □确保各部□公平性而随机确定的□程
Answer: (SHOW ANSWER)
The order of restoration defines a predefined, prioritized sequence for recovering systems and business functions following a disruption, based on their criticality and interdependencies as identified during the Business Impact Analysis, ensuring that the most essential functions-and the underlying infrastructure they depend on-are recovered first, given that available recovery resources, bandwidth, and personnel are typically constrained immediately following a disruptive event.

NEW QUESTION: 458

一家公司決定需要開始維護企業中部署的資口。
應採取什麼方法來確定和維護所有權資訊以使公司合規？
A. 企業資口管理框架
B. 使用商業現成軟體的資口基線
C. 使用網域登入記錄的資口所有權資料庫
D. 報告資口上的活動使用者登入的口本
Answer: A (LEAVE A REPLY)
The most appropriate approach for maintaining ownership information and ensuring compliance is:
A). Enterprise asset management framework
This approach provides a structured system to track, manage, and assign ownership of assets while ensuring the company remains compliant with relevant policies and regulations.

NEW QUESTION: 459
員工的家庭住址應依下列哪一項參考資料分類？
A. 員工簽署的同意書條款與條件
B. 組織的資料分類模型
C. 現有員工資料分類
D. 組織人力資源安全計劃
Answer: B (LEAVE A REPLY)
An employee's home address should be categorized according to the organization's data classification model. A data classification model is a framework for defining the sensitivity and criticality of data based on its value, impact, and legal requirements. A data classification model typically consists of different levels of data categories, such as public, internal, confidential, and restricted. An organization should apply a data classification model to all its data assets, including employee data, to ensure their proper protection, handling, and disposal. An employee's home address is a type of personal data that may be subject to privacy laws and regulations, such as the General Data Protection Regulation (GDPR). Therefore, an organization should classify an employee's home address according to its data classification model and assign appropriate controls and safeguards. The consent form terms and conditions signed by employees are not a reference for data classification, as they are not a standard or a policy. Existing employee data classifications are not a reference for data classification, as they are not a guideline or a criterion.
An organization security plan for human resources is not a reference for data classification, as it is not a framework or a scheme.

NEW QUESTION: 460
下列哪一種授權標準是為了處理聯合身分識別管理 (FIM) 的應用程式介面 (API) 存取而建構的？
A. 安全性斷言標記語言 (SAML)
B. 開放式身份驗證 (OAUTH)
C. 遠端驗證撥入使用者服務 (RADIUS)
D. 終端存取控制存取控制系統增強版 (TACACS+)
Answer: B (LEAVE A REPLY)

The authorization standard that is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM) is Open Authentication (OAuth). OAuth is a standard protocol that enables the delegation of authorization to access resources or services from one party to another, without sharing the credentials. OAuth can be used for FIM, which is a mechanism that allows the users to use a single identity across multiple domains or systems, such as social media platforms, cloud services, or web applications. OAuth can handle API access for FIM, which means that the users can authorize the applications to access their data or services from other providers, such as contacts, calendars, or photos, through the APIs. Security Assertion Markup Language (SAML), Remote Authentication Dial-in User Service (RADIUS), and Terminal Access Control Access Control System Plus (TACACS+) are not authorization standards that are built to handle API access for FIM, but they are standards or protocols that can be used or supported by FIM for authentication, authorization, or accounting purposes.

NEW QUESTION: 461
以下哪□最能描述“数据分□”？
A. 将□□数据□予□□价□的□程
B. 根据数据的敏感性及其未□授□披露的影响□数据□行分□，以便□用适当的保□□□。
C. □所有□□数据□行□一加密的□程
D. □除□□数据的□程
Answer: B (LEAVE A REPLY)
Data classification categorizes information (e.g., Public, Internal, Confidential, Restricted) based on its sensitivity and the potential impact of unauthorized disclosure, loss, or modification, enabling the organization to apply appropriate and proportionate security controls to protect each category of data.

NEW QUESTION: 462
多執行緒應用程式比單執行緒應用程式更容易受到攻擊
A. 競態條件。
B. 病毒感染。
C. 資料包嗅探。
D. 資料庫注入。
Answer: A (LEAVE A REPLY)
Multi-threaded applications are more at risk than single-threaded applications to race conditions.
A race condition is a type of concurrency error that occurs when two or more threads access or modify the same shared resource without proper synchronization or coordination. This may result in inconsistent, unpredictable, or erroneous outcomes, as the final result depends on the timing and order of the thread execution. Race conditions can compromise the security, reliability, and functionality of the application, and can lead to data corruption, memory leaks, deadlock, or privilege escalation.

NEW QUESTION: 463
以下哪□最能描述“欺□”□种攻□技□？

A. □求□多□致系□□□
B. □造数据，例如IP 地址或□子□件地址，以冒充可信□体
C. 截□和□改□□中的数据
D. 利用□件中的□□条件
Answer: (SHOW ANSWER)
Spoofing involves forging identifying information-such as a source IP address, MAC address, caller ID, or email sender address-to impersonate a trusted system or user, often used to bypass access controls or deceive victims in social engineering and network attacks.

NEW QUESTION: 464
下列哪些是針對被動網路層攻擊的有效對策？
A. 聯合安全性和經過驗證的存取控制
B. 可信任軟體開發與執行時間完整性控制
C. □用加密和安全的應用程式
D. Enclave邊界保護與運算環境防禦
Answer: C (LEAVE A REPLY)
Encryption ensures that data is transformed into a code that can only be accessed by authorized parties. Security-enabled applications ensure that only authorized users can access specific network resources, protecting against passive network-layer attacks like eavesdropping or sniffing.

NEW QUESTION: 465
下列哪項信任服務原則涉及向第三方提供者的客□提供的系統、□品或服務所使用的資訊的可存取性？
A. 安全
B. 隱私
C. 訪問
D. 可用性
Answer: D (LEAVE A REPLY)
Availability is the trust services principle that refers to the accessibility of information used by the systems, products, or services offered to a third-party provider's customers. Trust services principles are the criteria and guidelines that are used to evaluate and report on the controls and processes of a service organization, such as a cloud service provider, a data center, or a payroll service. Trust services principles are based on the standards and frameworks issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). There are five trust services principles: security, availability, processing integrity, confidentiality, and privacy. Availability is the trust services principle that addresses the ability of the service organization to ensure that the systems, products, or services are accessible and operational for use by the customers as agreed or expected. Availability can be measured by various metrics, such as uptime, downtime, response time, recovery time, or service level agreements.

NEW QUESTION: 466
下列哪個部門發起請求、批准和供應業務流程？

A. 操作
B. 人力資源 (HR)
C. 資訊科技 (IT)
D. 安全
Answer: B (LEAVE A REPLY)
The department that initiates the request, approval, and provisioning business process is human resources (HR). The request, approval, and provisioning business process is the process that involves requesting, approving, and provisioning the access rights and privileges for the users or employees of an organization, based on their roles and responsibilities. The HR department initiates the request, approval, and provisioning business process, as it is responsible for managing the human resources of the organization, and for ensuring that the users or employees have the appropriate access rights and privileges to perform their duties and functions. The HR department can initiate the request, approval, and provisioning business process by creating, updating, or terminating the user or employee accounts, and by communicating the access requirements and changes to the other departments, such as IT, security, or operations.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 467
下列哪一項是雙重認證的範例？
A. 視網膜掃描與掌紋
B. 指紋和智慧卡
C. 磁條卡和 ID 徽章
D. 區分電腦和人類的密碼和全自動公共圖靈測試 (CAPTCHA)
Answer: B (LEAVE A REPLY)
An example of two-factor authentication is fingerprint and a smart card. Two-factor authentication is a type of authentication that requires two different factors or methods to verify the identity or the credentials of a user or a device. The factors or methods can be categorized into three types: something you know, something you have, or something you are. Something you know is a factor that relies on the knowledge of the user or the device, such as a password, a PIN, or a security question. Something you have is a factor that relies on the possession of the user or the device, such as a smart card, a token, or a certificate. Something you are is a factor that relies on the biometrics of the user or the device, such as a fingerprint, a retina scan, or a voice recognition.
Fingerprint and a smart card are an example of two-factor authentication, as they combine two different factors:

something you are and something you have. Retina scan and a palm print are not an example of two-factor authentication, as they are both the same factor: something you are. Magnetic stripe card and an ID badge are not an example of two-factor authentication, as they are both the same factor: something you have. Password and CAPTCHA are not an example of two-factor authentication, as they are both the same factor: something you know.

NEW QUESTION: 468
下列哪一項是減少活動使用者工作站資料被盜的最有效方法？
A. 實施全碟加密
B. □用多重身份驗證
C. 部署檔案完整性檢□器
D. 禁止使用便攜式設備
Answer: D (LEAVE A REPLY)
The most effective method of mitigating data theft from an active user workstation is to disable use of portable devices. Portable devices are the devices that can be easily connected to or disconnected from a workstation, such as USB drives, external hard drives, flash drives, or smartphones. Portable devices can pose a risk of data theft from an active user workstation, as they can be used to copy, transfer, or exfiltrate data from the workstation, either by malicious insiders or by unauthorized outsiders. By disabling use of portable devices, the data theft from an active user workstation can be prevented or reduced.

NEW QUESTION: 469
以下哪□最能描述“出口点□□□□□估□□ (CAEP)”的目的？
A. □用于用□初始一次性身份□□的□□
B. 一种□□，支持跨集成系□□□ 事件□□地□□用□或会□□□或授□状□(例如□□禁用或□□到入侵)的重大□化信息，从而允□立即撤□或重新□估□□□限，而无需等待下一次令牌刷新
C. 一种□□用于加密静□数据的□□。
D. 一种□□□□令牌的方法
Answer: B (LEAVE A REPLY)
CAEP enables real-time, event-driven sharing of significant security-relevant changes-such as a detected account compromise, a user's termination, or a risk score change-across integrated systems and applications, allowing access to be immediately revoked or re-evaluated as conditions change, rather than relying solely on the natural expiration and periodic refresh cycle of a previously issued access token, aligning with Zero Trust and continuous authentication principles.

NEW QUESTION: 470
在允許 Web 應用程式進入生□環境之前，安全從業者會執行多種類型的測試以確認Web 應用程式按預期執行。為了測試使用者名字段，安全從業者創建了一個測試，在該欄位中輸入的字元數多於允許的字元數。下列哪一項最能描述所執行的測試類型？
A. 誤用案例測試

B. 滲透測試
C. 網路會話測試
D. 介面測試
Answer: A (LEAVE A REPLY)
Misuse case testing is the best term to describe the type of test performed by the security practitioner to test the username field. Misuse case testing is a type of testing that involves negative scenarios or malicious actions that may compromise the functionality or the security of the system. Misuse case testing is based on the concept of misuse cases, which are the opposite of use cases. Use cases are the normal or expected scenarios or interactions between the system and the users or the actors. Misuse cases are the abnormal or unexpected scenarios or interactions that may cause errors, failures, or attacks. For example, entering more characters into the username field than is allowed is a misuse case that may result in a buffer overflow or a denial-of-service attack.

NEW QUESTION: 471
點對點協定 (PPP) 使用下列哪一項來決定資料包格式？
A. 第 2 層隧道協定 (L2TP)
B. 鏈路控制協定 (LCP)
C. 質詢握手驗證協定 (CHAP)
D. 資料包傳輸協定 (PTP)
Answer: (SHOW ANSWER)
Link Control Protocol (LCP) is used by the Point-to-Point Protocol (PPP) to determine packet formats. PPP is a data link layer protocol that provides a standard method for transporting network layer packets over point-to-point links, such as serial lines, modems, or dial-up connections. PPP supports various network layer protocols, such as IP, IPX, or AppleTalk, and it can encapsulate them in a common frame format. PPP also provides features such as authentication, compression, error detection, and multilink aggregation. LCP is a subprotocol of PPP that is responsible for establishing, configuring, maintaining, and terminating the point-to- point connection. LCP negotiates and agrees on various options and parameters for the PPP link, such as the maximum transmission unit (MTU), the authentication method, the compression method, the error detection method, and the packet format. LCP uses a series of messages, such as configure-request, configure-ack, configure-nak, configure-reject, terminate-request, terminate- ack, code-reject, protocol-reject, echo-request, echo- reply, and discard-request, to communicate and exchange information between the PPP peers.

NEW QUESTION: 472
在本地環境與外部身分提供者服務之間實施安全性斷言標記語言 (SAML) 以實現身分整合時，常見的挑戰是什麼？
A. 部分使用者未獲得服務權限。
B. SAML 令牌由本機身分提供者提供。
C. 單一使用者無法從服務中撤銷。
D. SAML 令牌包含使用者資訊。

Answer: A (LEAVE A REPLY)

A common challenge when implementing SAML for identity integration between on-premise environment and an external identity provider service is that some users are not provisioned into the service. Provisioning is a process of creating, updating, or deleting the user accounts or profiles in a service or an application, based on the user identity or credentials. When implementing SAML for identity integration, the on-premise environment acts as the identity provider, which authenticates the user and issues the SAML assertion, and the external service acts as the service provider, which receives the SAML assertion and grants access to the user.

However, if the user account or profile is not provisioned or synchronized in the external service, the user may not be able to access the service, even if they have a valid SAML assertion.

Therefore, a common challenge when implementing SAML for identity integration is to ensure that the user provisioning is consistent and accurate between the on-premise environment and the external service. SAML tokens are provided by the on-premise identity provider, single users can be revoked from the service, and SAML tokens contain user information are not common challenges when implementing SAML for identity integration, as they are related to the functionality, granularity, or content of the SAML protocol, not the provisioning of the user accounts or profiles.

NEW QUESTION: 473

當筆記型電腦被竊時，下列哪一項措施能提供最有效的資料保護，防止敏感資訊被竊？

A. 設定 BIOS 和作業系統密碼

B. 加密用於儲存機密文件的虛擬磁碟機。

C. 實施強制性政策，規定敏感資料不得儲存在筆記型電腦上，而只能儲存在公司網路上

D. 加密整個磁碟，並在達到設定的存取失敗次數後刪除所有口容

Answer: (SHOW ANSWER)

Encrypting the entire disk and deleting the contents after a set number of failed access attempts provides the most protection against data theft of sensitive information when a laptop is stolen.

This method ensures that the data is unreadable without the correct decryption key, and that the data is erased if someone tries to guess the key or bypass the encryption. Setting up a BIOS and operating system password, encrypting the virtual drive, or implementing a policy are less effective methods, as they can be circumvented by physical access, booting from another device, or copying the data to another location.

NEW QUESTION: 474

什麼安全原則解決了 默默無聞的安全」問題？

A. 開放式設計

B. 職責分離 (SoD)

C. 基於角色的存取控制 (RBAC)

D. 最小權限

Answer: A (LEAVE A REPLY)

The security principle that addresses the issue of "Security by Obscurity" is open design. Open design is a principle that states that the security of a system or network should not depend on the secrecy or obscurity of its design, implementation, or configuration. Instead, the security of a system or network should rely on the strength and effectiveness of its security mechanisms, such as encryption, authentication, or access control. Open design is based on the assumption that the adversaries can access or discover the details and flaws of the system or network, and that the security mechanisms can withstand the scrutiny and attacks of the adversaries. Open design also encourages the sharing and review of the system or network design and implementation by the security community, which can help to identify and fix the vulnerabilities and improve the security quality. "Security by Obscurity" is a practice that contradicts the open design principle, and it involves hiding or concealing the details or weaknesses of the system or network, hoping that the adversaries will not find or exploit them. "Security by Obscurity" is considered ineffective and risky, because it provides a false sense of security, and it can be easily compromised or bypassed by the adversaries who have the tools and techniques to reveal or crack the secrets of the system or network.

NEW QUESTION: 475
建立有效的資訊安全意識計劃最重要的因素是什麼？
A. 獲得管理階層的支持。
B. 舉辦年度安全意識活動。
C. 強制進行安全訓練。
D. 在牆上懸掛資訊安全海報,
Answer: A (LEAVE A REPLY)
The most important factor in establishing an effective Information Security Awareness Program is to obtain management buy-in. Management buy-in is the support and commitment of the senior management or the executives of an organization for a project or an initiative, such as an Information Security Awareness Program. An Information Security Awareness Program is a program that educates and trains the employees or the users of an organization about the security policies, procedures, risks, and best practices, and aims to improve the security culture and behavior of the organization. Obtaining management buy-in is essential for establishing an effective Information Security Awareness Program, as it can help to define the goals and objectives of the program, allocate the resources and budget for the program, communicate the importance and value of the program, and monitor and evaluate the progress and outcomes of the program. Management buy-in can also help to demonstrate the leadership and accountability of the management, and to motivate and influence the employees or the users to participate and comply with the program. Conducting an annual security awareness event, mandating security training, and hanging information security posters on the walls are not the most important factors in establishing an effective Information Security Awareness Program. These are some of the methods or techniques that may be used to implement or deliver the Information Security Awareness Program, but they are not as crucial or influential as obtaining management buy-in. Conducting an annual security awareness event is a method that organizes a special event or a campaign once a year, to raise the awareness and knowledge of the employees or the users about the security topics or issues. Mandating security training is a method that requires the employees or the

users to attend or complete a formal or structured training course or session, to learn the security skills or competencies. Hanging information security posters on the walls is a method that displays or distributes visual or graphical materials, such as posters, flyers, or stickers, to remind or inform the employees or the users about the security messages or tips.

NEW QUESTION: 476
安全團隊的任務是針對前端外部應用程式執行介面測試，並且需要驗證所有輸入欄位是否可以防止無效輸入。下列哪一項最有助於此過程？
A. 應用程式模糊測試
B. 指令集模擬
C. 迴歸測試
D. 健全性測試
Answer: A (LEAVE A REPLY)
Application fuzzing is a testing technique used to identify vulnerabilities in an application by inputting random, unexpected, or malformed data into the input fields. The purpose of fuzzing is to test how the application handles invalid or unexpected inputs. This type of testing is particularly useful for detecting buffer overflows, input validation errors, and other security vulnerabilities that might be exploited by attackers.
In the context of verifying that all input fields protect against invalid input, fuzzing is highly effective because it automates the process of sending a wide range of random and invalid inputs to the application. It helps ensure that the application handles these inputs securely, without crashing or exposing sensitive information.

NEW QUESTION: 477
以下哪□最能描述“生成式人工智能工具的出口点数据□失防□”在工作□所中的用途？
A. 无□在何种情况下，都□禁止使用所有生成式人工智能工具。
B. □控和控制敏感或机密数据向外部生成式人工智能工具(例如公共聊天机器人)的提交，防止□有信息意外泄露□第三方人工智能提供商。
C. □人工智能工具生成的所有□出□行加密
D. 一种□□用于提高人工智能模型准确率的技□
Answer: (SHOW ANSWER)
DLP controls tailored for generative AI tools monitor and restrict the submission of sensitive, confidential, or regulated data into external, third-party generative AI platforms (such as public chatbots), addressing the risk that employees might inadvertently expose proprietary source code, customer data, or trade secrets to external AI providers, whose data handling and retention practices may not align with organizational security requirements.

NEW QUESTION: 478
請參考以下資訊回答問題。

一位新員工獲配一台擁有完整管理員權限的筆記型電腦。該員工家中沒有個人電腦，他的孩子會使用這台電腦收發電子郵件、上網和使用即時通訊工具。公司資訊科技部門發現，有人利用該員工的權限在電腦上安裝了一款點對點程式。
下列哪一份文件解釋了組織資□的正確使用方法？
A. 人力資源政策
B. 可接受使用政策
C. 道德準則
D. 存取控制策略
Answer: B (LEAVE A REPLY)
The document that explains the proper use of the organization's assets is the acceptable use policy. An acceptable use policy is a document that defines the rules and guidelines for the appropriate and responsible use of the organization's information systems and resources, such as computers, networks, or devices. An acceptable use policy can help to prevent or reduce the misuse, abuse, or damage of the organization's assets, and to protect the security, privacy, and reputation of the organization and its users. An acceptable use policy can also specify the consequences or penalties for violating the policy, such as disciplinary actions, termination, or legal actions. A human resources policy, a code of ethics, and an access control policy are not the documents that explain the proper use of the organization's assets, as they are related to the management, values, or authorization of the organization's employees or users, not the usage or responsibility of the organization's information systems or resources.

NEW QUESTION: 479
在前往高風險國家/地區時，下列哪項措施是保護電腦 智慧型手機和外部儲存裝置上的資料的最佳方法？
A. □看適用的目的地國家/地區法律，在旅行前對設備進行取證清理，並且僅在到達目的地後透過虛擬專用網路 (VPN) 下載敏感資料。
B. 不使用時將筆記型電腦、外部儲存裝置和智慧型手機存放在飯店房間□。
C. 利用虛擬私人網路 (VPN) 上的安全通訊端層 (SSL) 連線在到達目的地後下載敏感資料。
D. 使用多重身份驗證 (MFA) 來存取儲存在筆記型電腦或外部儲存裝置上的數據，並使用生物識別指紋存取控制機制來解鎖智慧型手機。
Answer: A (LEAVE A REPLY)
The best measure for protecting data on devices when traveling to high-risk countries is to review the applicable destination country laws, forensically clean the devices prior to travel, and only download sensitive data over a VPN upon arriving at the destination. This will minimize the risk of data loss, theft, or compromise due to border inspections, device confiscation, malware infection, or network interception. Keeping devices in the hotel room, using SSL or VPN connections, or using MFA or biometric access controls may not be sufficient or effective in protecting data in high-risk countries, as they may still be subject to physical or logical attacks by adversaries.

NEW QUESTION: 480
下列哪一項的年化預期損失(ALE)較高？

Event	Loss Expectancy	Annualized Rate of Occurrence	Insurance Coverage
Fire	$1,000,000	0.1	80%
Flood	$250,000	0.2	50%
Windstorm	$50,000	0.5	80%
Earthquake	$800,000	0.02	None

A. 火災
B. 地震
C. 風暴
D. 洪水
Answer: B (LEAVE A REPLY)
Earthquake would present the higher annualized loss expectancy (ALE) according to the table in the image. ALE is a metric that measures the expected loss per year due to a specific risk or threat. ALE is calculated by multiplying the single loss expectancy (SLE), which is the estimated cost of a single occurrence of the risk or threat, by the annualized rate of occurrence (ARO), which is the estimated frequency of the risk or threat occurring in a year. According to the table, the ALE for each event is as follows:
Fire: $1,000,000 x 0.1 = $100,000
Flood: $250,000 x 0.2 = $50,000
Windstorm: $50,000 x 0.5 = $25,000
Earthquake: $800,000 x 0.02 = $16,000
Therefore, earthquake has the highest ALE of $16,000, followed by fire, flood, and windstorm.
Note that the insurance coverage does not affect the ALE calculation, as it only reduces the actual loss, not the expected loss. However, insurance coverage can be used to reduce the total cost of risk (TCOR), which is the sum of ALE and the cost of risk mitigation, such as insurance premiums, deductibles, and administrative costs.

NEW QUESTION: 481
下列哪一項是需要係統重新認證和重新認可的主要原因？
A. 幫助資料擁有者做出未來的敏感度和關鍵性確定
B. 向軟體開發團隊保證所有安全問題都已解決
C. 驗證組織安全策略是否仍可接受安全保護
D. 幫助安全團隊接受或拒□新系統的實施與生□
Answer: C (LEAVE A REPLY)
The main reason that system re-certification and re-accreditation are needed is to verify that the security protection of the system remains acceptable to the organizational security policy, especially after significant changes or updates to the system. Re-certification is the process of reviewing and testing the security controls of the system to ensure that they are still effective and compliant with the security policy. Re-accreditation is the process of authorizing the system to operate based on the results of the re-certification.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 482
作為最佳實踐，安全評估報告(SAR) 應包括下列哪些部分？
A. 資料分類策略
B. 軟體與硬體清單
C. 修復建議
D. 參與者姓名
Answer: C (LEAVE A REPLY)
A Security Assessment Report (SAR) is a document that summarizes the findings and recommendations of a security assessment. A SAR should include the following sections: an executive summary, a scope and methodology, a threat and risk analysis, a vulnerability analysis, a security control assessment, and remediation recommendations. Remediation recommendations are the best practices that the SAR should include, as they provide the actions that need to be taken to address the identified security gaps and risks. Data classification policy, software and hardware inventory, and names of participants are not essential sections of a SAR, although they may be included as supporting information or appendices.

NEW QUESTION: 483
以下哪□是□防性行政控制的最佳示例？
A. 一扇上□的服□器机房□
B. 入□前背景□□
C. 入侵□□系□
D. □路□□(CCTV)□像机
Answer: B (LEAVE A REPLY)
A pre-employment background check is an administrative control that helps prevent hiring individuals who may pose a security risk, acting before an incident occurs. Locked doors and CCTV are physical controls, while an IDS is a technical (and largely detective) control.

NEW QUESTION: 484
以下哪□最能描述“商□□子□件□□ (BEC)”？
A. □□□子□件服□器□件漏洞的技□攻□
B. 一种社会工程攻□，攻□者通□□子□件冒充受信任的高管 供□商或合作伙伴，□□□工□行欺□性付款或泄露敏感信息。
C. 一种加密□子□件通信的方法

D. 一种完全依□□意□子□件附件的攻□

Answer: B (LEAVE A REPLY)

BEC is a social engineering attack in which an attacker impersonates a trusted individual (such as a CEO, CFO, or known vendor)-often through a spoofed or compromised email account-to deceive an employee into transferring funds, changing payment details, or disclosing sensitive information, typically without relying on malware or technical exploits, instead leveraging trust and urgency.

NEW QUESTION: 485

商業現成 (COTS) 軟體有下列哪些額外的安全性問題？

A. 供應商對 COTS 軟體漏洞負責。

B. □部開發的軟體本質上安全性較低。

C. COTS 軟體的漏洞有詳細記錄並公開可用。

D. COTS 軟體本質上較不安全。

Answer: (SHOW ANSWER)

Commercial off-the-shelf (COTS) software is a type of software that is readily available for purchase from a vendor or a third party, and that can be used with little or no modification. COTS software is often cheaper, faster, and easier to acquire and deploy than custom or in-house developed software, as it does not require extensive development, testing, or maintenance efforts. However, COTS software also presents some additional security concerns, such as:

Exploits for COTS software are well documented and publicly available. COTS software is widely used by many organizations and individuals, which makes it an attractive target for attackers.

Moreover, the vulnerabilities and exploits for COTS software are often disclosed and published by security researchers, vendors, or hackers, which makes them accessible to anyone who wants to exploit them. Therefore, COTS software users need to apply the security patches and updates provided by the vendors as soon as possible, and monitor the security advisories and bulletins for any new threats or issues.

Vendors may not provide adequate support or updates for COTS software. COTS software users depend on the vendors or the third parties for the security and functionality of the software.

However, the vendors may not provide timely or sufficient support or updates for the software, especially if the software is outdated, discontinued, or unsupported. This may leave the users with unpatched or insecure software, which can expose them to various risks and attacks.

Therefore, COTS software users need to evaluate the vendor's reputation, track record, and service level agreements, and ensure that the software is compatible and compliant with their security requirements and standards.

COTS software may not meet the specific needs or expectations of the users. COTS software is designed to meet the general or common needs of a broad range of users, which may not match the specific or unique needs or expectations of some users. For example, COTS software may not have the desired features, functions, or performance that the users require, or it may have some unwanted or unnecessary features, functions, or components that the users do not need.

This may result in reduced efficiency, productivity, or satisfaction for the users, or increased complexity, overhead, or waste for the system. Therefore, COTS software users need to conduct a thorough

analysis and evaluation of the software before purchasing or deploying it, and ensure that it meets their business and technical objectives and criteria.

NEW QUESTION: 486
緊急應變計畫演練旨在達到下列哪些目的？
A. 培訓人員的角色與職責
B. 驗證服務等級協定
C. 列車維修人員
D. 驗證營運指標
Answer: A (LEAVE A REPLY)
Contingency plan exercises are intended to train personnel in roles and responsibilities.
Contingency plan exercises are simulated scenarios that test the preparedness and effectiveness of the contingency plan, which is a document that outlines the actions and procedures to be followed in the event of a disruption or disaster. Contingency plan exercises help to train the personnel involved in the contingency plan, such as the incident response team, the recovery team, and the business continuity team, in their roles and responsibilities, such as communication, coordination, decision making, and execution. Contingency plan exercises also help to identify and resolve any issues or gaps in the contingency plan, and to improve the skills and confidence of the personnel.

NEW QUESTION: 487
硬體保留策略應包含下列哪些口容？
A. 在保留敏感資料之前使用加密技術對其進行加密。
B. 資料僅保留一周，並將資料保留工作外包給第三方供應商
C. 將所有敏感資料保留在媒體和硬體上
D. 僅保留出於業務目的所需資料的計劃和保留時間表
Answer: D (LEAVE A REPLY)
A hardware retention policy is a set of guidelines that defines how long hardware and data should be kept and how they should be disposed of when they are no longer needed. A hardware retention policy should include a plan to retain data required only for business purposes and a retention schedule that specifies the duration and frequency of data retention. This can help to reduce the risk of data breaches, comply with legal and regulatory requirements, optimize storage space and costs, and support business continuity and disaster recovery. A hardware retention policy should also include procedures for secure data erasure and hardware disposal to prevent unauthorized access to sensitive data.

NEW QUESTION: 488
認證的主要目的是：
A. 遵守適用的法律和法規。
B. 允許高階管理層就是否接受作業系統風險做出明智的決定。
C. 保護組織的敏感資料。

D. 驗證所有安全控制是否已正確實施並以正確的方式運作。

Answer: B (LEAVE A REPLY)

According to the CISSP CBK Official Study Guide, the primary purpose of accreditation is to allow senior management to make an informed decision regarding whether to accept the risk of operating the system. Accreditation is the process of formally authorizing a system to operate based on the results of the security assessment and the risk analysis. Accreditation is a management responsibility that involves evaluating the security posture, the residual risk, and the compliance status of the system, and determining if the system is acceptable to operate within the organization's risk tolerance. Accreditation does not necessarily mean that the system complies with applicable laws and regulations, protects the organization's sensitive data, or verifies that all security controls have been implemented properly and are operating in the correct manner, although these may be factors that influence the accreditation decision.

NEW QUESTION: 489

下列何者最能描述恢復時間目標 (RTO)？

A. 災難發生後資料驗證的時間

B. 災難發生後從備份還原資料的時間

C. 災難發生後應用程式復原的時間

D. 災難發生後應用程式驗證的時間

Answer: C (LEAVE A REPLY)

The best description of Recovery Time Objective (RTO) is the time of application resumption after disaster. RTO is a metric that defines the maximum acceptable time that an application or a system can be unavailable or offline after a disaster or a disruption. RTO is based on the business impact analysis and the recovery requirements of the organization, and it helps to determine the recovery strategies and the resources needed to restore the application or the system to its normal operation. Time of data validation after disaster, time of data restoration from backup after disaster, and time of application verification after disaster are not the best descriptions of RTO, as they are related to the quality, accuracy, or completeness of the data or the application, not the availability or the downtime of the application or the system.

NEW QUESTION: 490

變更管理政策和程序屬於下列哪一種類型的控制？

A. 指令

B. 偵探

C. 修正

D. 預防

Answer: (SHOW ANSWER)

Change management policies and procedures belong to the type of controls that are directive. Controls are the measures and the mechanisms that are used to protect and safeguard the organization's information systems and assets, and to ensure that they comply with the organization's security and business objectives. Controls can be classified into different types, based on their

purpose, function, or nature, such as preventive, detective, corrective, deterrent, compensating, or recovery controls. Directive controls are the type of controls that guide and regulate the actions and the behaviors of the organization's staff, processes, and systems, and that ensure that they follow the organization's policies, standards, and regulations. Directive controls can include policies, procedures, guidelines, standards, rules, regulations, laws, or contracts. Change management policies and procedures belong to the type of controls that are directive, as they provide the instructions and the requirements for managing and controlling any changes to the organization's information systems and assets, and for ensuring that the changes align with the organization's security and business requirements.

NEW QUESTION: 491
如果要使用入侵防禦系統 (IPS) 的防禦功能，建議的感測器配置模式是什麼？
A. 活動
B. 被動
C. 口聯
D. 跨度
Answer: (SHOW ANSWER)
Inline is the recommended configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used. An IPS is a network security device that monitors and analyzes the network traffic for malicious or anomalous activities, and takes actions to block or stop them. An IPS sensor is the component that performs the detection and prevention functions of the IPS. An IPS sensor can be configured in different modes, such as active, passive, inline, or span. Inline mode means that the IPS sensor is placed directly in the network traffic path, and can modify, drop, or redirect the packets as they pass through. Inline mode enables the IPS sensor to use its prevention capabilities effectively, as it can stop the attacks in real time, before they reach their intended targets.

NEW QUESTION: 492
以下哪口最能描述灾口恢复口划中“口用站点”的用途？
A. 配口口全、人口充足的口施，可口行口口数据复制
B. 部分口口已配口，部分硬件和口接已就口，但需要口外口置和数据恢复才能投入使用
C. 口配口口力和暖通空口系口的空置厂房，需要采口和安装所有口口。
D. 口口用于存档数据存口的口施
Answer: B (LEAVE A REPLY)
A warm site is a partially configured alternate facility that has some hardware, network connectivity, and infrastructure in place but requires additional steps-such as installing remaining equipment and restoring data from backups-before it can support operations, offering a middle ground between the cost of a hot site and the slower recovery of a cold site.

NEW QUESTION: 493
下列哪一個模型使用唯一衝突類別中包含的唯一組？
A. 中國牆

B. 貝爾拉帕杜拉
C. 克拉克威爾遜
D. 比巴
Answer: A (LEAVE A REPLY)
The Chinese Wall model is a security model designed to prevent conflicts of interest within an organization by using conflict classes and unique groups. It is often used in environments like financial institutions, where there is a need to ensure that employees or contractors working with one client cannot access sensitive information related to a competing client.
In the Chinese Wall model:
Conflict classes are groups of objects that, if accessed, could create a conflict of interest. These objects belong to unique groups that are designed to prevent users from accessing information that could lead to a conflict of interest.
The model ensures that once a user accesses a piece of information within a certain conflict class, they are restricted from accessing data from a competing or conflicting conflict class.

NEW QUESTION: 494
以下哪□最能描述"□深防御"原□？
A. 依靠□一、高效的安全控制
B. 采用多□互□的安全控制措施，即使其中一□失效，其他措施仍能提供保□
C. 将所有安全□能外包□第三方
D. □将安全投□集中于周界防御
Answer: B (LEAVE A REPLY)
Defense in depth is a layered security strategy that employs multiple overlapping controls (physical, technical, and administrative) across different levels of the environment, so that the failure or bypass of a single control does not result in a complete security breach.

NEW QUESTION: 495
請參考以下資訊回答問題。
在對一起安全事件進行調□的過程中，確定有未經授權的個人存取了託管包含財務資訊的資料庫的系統。如果發現大量資訊已被未經授權的個人複製，那麼資料的哪個屬性受到了損害？
A. 可用性
B. 完整性
C. 問責制
D. 保密性
Answer: (SHOW ANSWER)
The attribute of the data that has been compromised, if it is discovered that large quantities of information have been copied by the unauthorized individual, is the confidentiality. The confidentiality is the property or the characteristic of the data that ensures that the data is only accessible or disclosed to the authorized individuals or entities, and that the data is protected from the unauthorized or the malicious access or disclosure. The confidentiality of the data can be compromised when the data is

copied, stolen, leaked, or exposed by an unauthorized individual or a malicious actor, such as the one who accessed the system hosting the database.
The compromise of the confidentiality of the data can violate the privacy, the rights, or the interests of the data owners, subjects, or users, and can cause damage or harm to the organization's operations, reputation, or objectives. Availability, integrity, and accountability are not the attributes of the data that have been compromised, if it is discovered that large quantities of information have been copied by the unauthorized individual, as they are related to the accessibility, the accuracy, or the responsibility of the data, not the secrecy or the protection of the data.

NEW QUESTION: 496
如果發生同步 (SYN) 洪水攻擊，開放系統互連(OSI) 模型的哪一層將成為攻擊目標？
A. 會話
B. 運輸
C. 網絡
D. 演示
Answer: B (LEAVE A REPLY)
A Synchronization (SYN) flood attack is a type of denial-of-service (DoS) attack that exploits the three-way handshake mechanism of the Transmission Control Protocol (TCP), which operates at the transport layer of the Open Systems Interconnection (OSI) model. In a SYN flood attack, the attacker sends a large number of SYN packets to the target server, but does not respond to the SYN-ACK packets sent by the server. This causes the server to exhaust its resources and become unable to accept legitimate requests. The session, network, and presentation layers of the OSI model are not directly involved in this attack.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 497
私有和公用加密金鑰的使用對於實現下列哪一項至關重要？
A. Diffie-Hellman 演算法
B. 安全通訊端層 (SSL)
C. 進階加密標準 (AES)
D. 訊息摘要 5 (MD5)
Answer: (SHOW ANSWER)

The use of private and public encryption keys is fundamental in the implementation of Secure Sockets Layer (SSL). SSL is a protocol that provides secure communication over the Internet by using public key cryptography and digital certificates. SSL works as follows:
The client initiates a connection to the server and requests its digital certificate, which contains its public key and identity information.
The server sends its digital certificate to the client, and optionally requests the client's digital certificate as well.
The client verifies the server's digital certificate with a trusted third party, such as a certificate authority (CA), and optionally sends its own digital certificate to the server.
The server verifies the client's digital certificate with a trusted third party, if applicable.
The client and the server use the Diffie-Hellman algorithm to generate a shared secret key, which is used to encrypt and decrypt the data exchanged between them.
The client and the server use the shared secret key and a symmetric encryption algorithm, such as Advanced Encryption Standard (AES), to establish a secure session and communicate confidentially and reliably.
The use of private and public encryption keys is fundamental in the implementation of SSL because it enables the authentication of the parties, the establishment of the shared secret key, and the protection of the data from eavesdropping, tampering, and replay attacks.

NEW QUESTION: 498
下列哪一項負責因外包資訊科技 (IT) 系統和服務而對組織系統和資料造成的風險？
A. 收購組織
B. 服務提供者
C. 風險主管（職能）
D. IT 經理
Answer: A (LEAVE A REPLY)
The acquiring organization is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services. Outsourcing is the practice of contracting out a business function or process to a third-party provider, such as a cloud service provider, a data center, or a managed service provider. Outsourcing can offer various benefits to the acquiring organization, such as cost reduction, efficiency improvement, scalability enhancement, and expertise access. However, outsourcing also introduces various risks to the organizational systems and data, such as loss of control, dependency, compliance issues, service quality issues, and security breaches. The acquiring organization is ultimately responsible and accountable for the risk management of the outsourced IT systems and services, as it owns the systems and data and bears the consequences of any adverse events. The acquiring organization should perform due diligence, risk assessment, contract negotiation, service level agreement, monitoring, and auditing of the service provider, and ensure that the service provider meets the security and performance requirements and standards of the acquiring organization.

NEW QUESTION: 499

下列哪一種滅火方法既環保又最適合資料中心？
A. 惰性氣體滅火系統
B. 哈龍氣體滅火系統
C. 乾管噴頭
D. 濕管噴頭
Answer: (SHOW ANSWER)
In a data center, it's critical to choose a fire suppression system that protects both the hardware and the environment. An inert gas fire suppression system is an environmentally friendly and effective method for suppressing fires in data centers because it uses gases like argon, nitrogen, or carbon dioxide that do not harm sensitive electronic equipment. These gases work by reducing the oxygen levels in the protected area to the point where combustion is no longer sustainable, without causing harm to the environment.
Inert gas systems are preferable in environments like data centers because:
They are non-toxic to humans in moderate concentrations (although people must evacuate before levels drop too low).
They do not leave residue or cause damage to electronic equipment, unlike water-based systems that can cause corrosion.
They have a low environmental impact, especially compared to older systems like Halon.

NEW QUESTION: 500
災難復原計畫 (DRP) 的復原優先順序是基於下列哪些文件？
A. 服務等級協定 (SLA)
B. 業務連續性計劃 (BCP)
C. 業務影響分析 (BIA)
D. 危機管理計劃
Answer: C (LEAVE A REPLY)
According to the CISSP All-in-One Exam Guide, the restoration priorities of a Disaster Recovery Plan (DRP) are based on the Business Impact Analysis (BIA). A DRP is a document that defines the procedures and actions to be taken in the event of a disaster that disrupts the normal operations of an organization. A restoration priority is the order or sequence in which the critical business processes and functions, as well as the supporting resources, such as data, systems, personnel, and facilities, are restored after a disaster. A BIA is a process that assesses the potential impact and consequences of a disaster on the organization's business processes and functions, as well as the supporting resources. A BIA helps to identify and prioritize the critical business processes and functions, as well as the recovery objectives and time frames for them. A BIA also helps to determine the dependencies and interdependencies among the business processes and functions, as well as the supporting resources. Therefore, the restoration priorities of a DRP are based on the BIA, as it provides the information and analysis that are needed to plan and execute the recovery strategy. A Service Level Agreement (SLA) is not the document that the restoration priorities of a DRP are based on, although it may be a factor that influences the restoration priorities. An SLA is a document that defines the expectations and requirements for the quality and performance of a service or product that is provided by a service

provider to a customer or client, such as the availability, reliability, scalability, or security of the service or product. An SLA may help to justify or support the restoration priorities of a DRP, but it does not provide the information and analysis that are needed to plan and execute the recovery strategy. A Business Continuity Plan (BCP) is not the document that the restoration priorities of a DRP are based on, although it may be a document that is aligned with or integrated with a DRP. A BCP is a document that defines the procedures and actions to be taken to ensure the continuity of the essential business operations during and after a disaster. A BCP may cover the same or similar business processes and functions, as well as the supporting resources, as a DRP, but it focuses on the continuity rather than the recovery of them. A BCP may also include other aspects or components that are not covered by a DRP, such as the prevention, mitigation, or response to a disaster. A crisis management plan is not the document that the restoration priorities of a DRP are based on, although it may be a document that is aligned with or integrated with a DRP. A crisis management plan is a document that defines the procedures and actions to be taken to manage and resolve a crisis or emergency situation that may affect the organization, such as a natural disaster, a cyberattack, or a pandemic. A crisis management plan may cover the same or similar business processes and functions, as well as the supporting resources, as a DRP, but it focuses on the management rather than the recovery of them. A crisis management plan may also include other aspects or components that are not covered by a DRP, such as the communication, coordination, or escalation of the crisis or emergency situation.

NEW QUESTION: 501
在進行安全風險評估時，下列哪一種類型的安全測試最能有效反映組織日常面臨的安全挑戰？
A. 外部
B. 公開
C. 口部
D. 隱蔽
Answer: C (LEAVE A REPLY)
The type of security testing that is the most effective in providing a better indication of the everyday security challenges of an organization when performing a security risk assessment is internal. Internal security testing is a type of security testing or a evaluation technique or method that assesses or analyzes the security or the protection of the system or the service from the perspective or the viewpoint of the insider or the authorized user or device within the organization, such as the employee, the contractor, or the partner, who has the legitimate or the valid access or permission to the system or the service, and who may pose or present the threat or the risk to the system or the service, intentionally or unintentionally, such as by exploiting or taking advantage of the vulnerabilities or the weaknesses of the system or the service, by misusing or abusing the access or the permission to the system or the service, or by being compromised or breached by the third parties or the attackers. Internal security testing can provide a better indication of the everyday security challenges of an organization when performing a security risk assessment, as it can reflect or represent the realistic or the practical scenario or situation of the security or the protection of the system or the service, by considering or taking into account the factors or the elements that affect or influence the security or the protection of the system or the service from the inside or the within the organization, such as the

policies, the procedures, the controls, the culture, or the behavior, and by identifying or detecting the vulnerabilities or the weaknesses of the system or the service that may be exploited or taken advantage of by the insider or the authorized user or device within the organization, such as the employee, the contractor, or the partner, who has the legitimate or the valid access or permission to the system or the service, and who may pose or present the threat or the risk to the system or the service, intentionally or unintentionally, such as by exploiting or taking advantage of the vulnerabilities or the weaknesses of the system or the service, by misusing or abusing the access or the permission to the system or the service, or by being compromised or breached by the third parties or the attackers.

NEW QUESTION: 502
下列哪一項是 Secure Shell (SSH) 的優點？
A. 運作在網路層。
B. 它對傳輸的使用者 ID 和密碼進行加密。
C. 它使用質詢回應來驗證各方的身分。
D. 它使用國際資料加密演算法（IDEA）來保護資料隱私
Answer: (SHOW ANSWER)
Secure Shell (SSH) is a network protocol that provides a secure and encrypted communication channel between two hosts over an unsecured network, such as the internet. SSH can be used for various purposes, such as remote login, file transfer, or command execution. One of the advantages of SSH is that it encrypts transmitted User ID and passwords. User ID and passwords are the common credentials that are used to authenticate the hosts or users involved in the communication. User ID and passwords are often transmitted in plain text over the network, which makes them vulnerable to various threats, such as interception, disclosure, or modification.
SSH can prevent these threats by encrypting the User ID and passwords using a symmetric key, which is generated and exchanged using a public key cryptography algorithm, such as RSA or DSA. SSH can also encrypt the entire communication using the same symmetric key, which provides additional security and privacy for the data. SSH can help to protect the User ID and passwords from various threats by encrypting them, as well as by using various security features, such as authentication, integrity, and certificates. It operates at the network layer, it uses challenge-response to authenticate each party, or it uses the International Data Encryption Algorithm (IDEA) for data privacy are not the advantages of SSH, as they are either incorrect, incomplete, or outdated statements about SSH.

NEW QUESTION: 503
下列何者最能描述業務影響分析 (BIA) 的目標？
A. 辨識可能對組織□生不利影響的事件和環境因素
B. 根據可能影響組織的干擾來確定重要和關鍵的□容。
C. 根據可能影響組織的威脅來確定業務連續性計劃 (BCP) 的需求
D. 準備計劃以建立執行業務連續性計劃 (BCP) 的組織意識
Answer: (SHOW ANSWER)

A Business Impact Analysis (BIA) is a key process in business continuity planning. The primary goal of the BIA is to identify and assess the impact of disruptions on critical business functions and processes. By determining what is most important and critical to the organization, it helps in prioritizing resources, recovery efforts, and planning for continuity in case of disruption.

NEW QUESTION: 504
符合歐盟美國安全港協議的隱私權政策必須包含下列哪些要素？
A. 口明資料主體收集的資訊將保留多長時間以及最終將如何處置。
B. 口明如果資料主體需要更正訊息，可以聯繫收集資訊的組織中的哪些人。
C. 資訊收集組織所遵循的監管架構和合規標準的解釋。
D. 對收集組織在收集資料主體資訊時所採用的所有技術的解釋。
Answer: B (LEAVE A REPLY)
The EU-US Safe Harbor Privacy Policy is a framework that was established in 2000 to enable the transfer of personal data from the European Union to the United States, while ensuring adequate protection of the data subject's privacy rights. The framework was invalidated by the European Court of Justice in 2015, and replaced by the EU-US Privacy Shield in 2016. However, the Safe Harbor Privacy Policy still serves as a reference for the principles and requirements of data protection across the Atlantic. One of the elements that a compliant Safe Harbor Privacy Policy must contain is an explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject. This is part of the principle of access, which states that individuals must have access to their personal information and be able to correct, amend, or delete it where it is inaccurate.

NEW QUESTION: 505
在處理支付卡口業資料安全標準 (PCI-DSS) 合規性問題時，與服務提供者共享持卡人資訊的組織必須執行下列哪項操作？
A. 每年對服務提供者進行 PCI-DSS 評估。
B. 定期驗證服務提供者的 PCI-DSS 合規狀態。
C. 驗證服務提供者的安全策略是否與組織的策略一致。
D. 確保服務提供者每年更新並測試其災難復原計畫(DRP)。
Answer: B (LEAVE A REPLY)
The action that an organization that shares card holder information with a service provider must do when dealing with compliance with the Payment Card Industry-Data Security Standard (PCI- DSS) is to validate the service provider's PCI-DSS compliance status on a regular basis. PCI- DSS is a set of security standards that applies to any organization that stores, processes, or transmits card holder data, such as credit or debit card information. PCI-DSS aims to protect the card holder data from unauthorized access, use, disclosure, or theft, and to ensure the security and integrity of the payment transactions. If an organization shares card holder data with a service provider, such as a payment processor, a hosting provider, or a cloud provider, the organization is still responsible for the security and compliance of the card holder data, and must ensure that the service provider also meets the PCI-

DSS requirements. The organization must validate the service provider's PCI-DSS compliance status on a regular basis, by obtaining and reviewing the service provider's PCI-DSS assessment reports, such as the Self-Assessment Questionnaire (SAQ), the Report on Compliance (ROC), or the Attestation of Compliance (AOC).
Performing a service provider PCI-DSS assessment on a yearly basis, validating that the service provider's security policies are in alignment with those of the organization, and ensuring that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis are not the actions that an organization that shares card holder information with a service provider must do when dealing with compliance with PCI-DSS, as they are not sufficient or relevant to verify the service provider's PCI-DSS compliance status or to protect the card holder data.

NEW QUESTION: 506
下列哪一項是受變更影響的個人或團體的名稱？
A. 變革推動者
B. 利害關係人
C. 贊助商
D. 最終用口
Answer: B (LEAVE A REPLY)
A stakeholder is the name of an individual or group that is impacted by a change. A stakeholder can be anyone who has an interest, influence, or dependency on the outcome of the change, such as the customers, users, employees, managers, suppliers, or regulators. A stakeholder can be affected positively or negatively by the change, and may have different expectations, needs, or concerns regarding the change. Therefore, it is important to identify, analyze, and engage the stakeholders throughout the change management process, and to communicate, consult, and collaborate with them effectively. A change agent is the name of an individual or group that initiates, sponsors, or implements the change. A change agent can be an internal or external party that has the authority, resources, or skills to drive the change and overcome the resistance.
A sponsor is the name of an individual or group that provides the strategic direction, funding, and support for the change. A sponsor is usually a senior executive or a leader who has the power and influence to champion the change and ensure its alignment with the organizational vision and goals. An end user is the name of an individual or group that uses the product, service, or system that is subject to the change. An end user is a type of stakeholder, but not all stakeholders are end users.

NEW QUESTION: 507
下列哪一項是讓路由器能口過濾 Internet 流量的標準存取控制清單 (ACL) 元素？
A. 媒體存取控制 (MAC) 位址
B. 網際網路通訊協定 (IP) 位址
C. 安全角色
D. 裝置需求
Answer: B (LEAVE A REPLY)

An Internet Protocol (IP) address is a standard Access Control List (ACL) element that enables a router to filter Internet traffic. An ACL is a set of rules that defines which packets are allowed or denied to pass through a router interface. An IP address is a numerical identifier that is assigned to each device on a network. By using IP addresses as ACL elements, a router can filter traffic based on the source or destination of the packets. For example, a router can block traffic from a specific IP address or allow traffic to a specific IP address.

NEW QUESTION: 508
一家醫院允許遠端資料庫開發人員存取虛擬私人網路 (VPN)。
在審核口部防火牆配置後，網路管理員發現分離隧道已口用。這個配置有什麼問題？
A. 遠端會話不需要多層身份驗證。
B. 允許遠端客口端與公用和專用網路交換流量。
C. 在特定情況下可能會利用多個 Internet 協定安全性 (IPSec) 隧道。
D. 網路入侵偵測系統 (NIDS) 將無法檢口安全通訊端層 (SSL) 流量。
Answer: B (LEAVE A REPLY)
Split-tunneling is a configuration that allows remote clients to access both the public and private network simultaneously through a VPN connection. This poses a security concern, because it increases the attack surface and exposes the private network to potential threats from the public network. Remote sessions may still require multi-layer authentication, multiple IPSec tunnels may not be exploitable in specific circumstances, and the NIDS may still inspect SSL traffic, depending on the VPN configuration.

NEW QUESTION: 509
下列哪一種方法是防止結構化口詢語言(SQL)注入的最佳方法？
A. 強制執行邊界檢口。
B. SELECT 指令的 Ratfrict um。
C. 限制超文本標記語言 (HTML) 原始碼
D. 使用預存程序。
Answer: (SHOW ANSWER)
Structured Query Language (SQL) injection is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL commands on a database server. SQL injection can result in data theft, data corruption, unauthorized access, or denial of service. The best way to protect against SQL injection is to use stored procedures, which are precompiled and parameterized SQL statements that are stored on the database server. Stored procedures prevent SQL injection by separating the user input from the SQL code, and by validating and sanitizing the user input before executing the SQL statement. Stored procedures also improve the performance and maintainability of the web application, as they reduce the network traffic and the code complexity. Other ways to protect against SQL injection are to enforce boundary checking, which limits the length and format of the user input, to restrict the use of SELECT command, which retrieves data from the

database, and to restrict the HyperText Markup Language (HTML) source code, which displays the web page content.

NEW QUESTION: 510
在使用最佳實踐從潛在犯罪現場收集數位證據時，數位調口員要做的第一步是什麼？
A. 諮詢主要調口人員，以了解案件的詳細資訊和所需的證據
B. 確保遵循接地程序，以減少因靜電放電導致的數位資料遺失
C. 更新用於確保證據可接受性的任何工具的基本輸入輸出系統 (BIOS) 和作業系統 (OS)。
D. 確認已向調口對象發出適當的搜索令，以消除非法搜索索賠
Answer: D (LEAVE A REPLY)
The first step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene is to confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims. A warrant is a legal document that authorizes the investigator to search, seize, or examine a person, place, or thing for evidence of a crime. A warrant is required to ensure that the investigation complies with the law and respects the rights and privacy of the subject. A warrant also prevents the evidence from being challenged or excluded in court due to illegal search or seizure.

NEW QUESTION: 511
下列何者最能描述集中式身分識別管理？
A. 服務提供者依賴受信任的第三方 (TTP) 向請求者提供憑證和識別碼。
B. 服務提供者同意跨組織邊界整合身分系統識別。
C. 服務提供者透過行為分析與識別因素來識別實體。
D. 服務提供者同時充當憑證和身分提供者 (IdP)。
Answer: D (LEAVE A REPLY)
The description that best describes centralized identity management is that service providers perform as both the credential and identity provider (IdP). Identity management is a type of process that involves defining, verifying, and managing the identity or the information of the users or the entities that access or use a system or a network, or a service or an application, using various methods, such as credentials, identifiers, or attributes. Identity management can provide various benefits, such as enhancing the security, functionality, or usability of the system or the network, or of the service or the application, and ensuring the compliance or alignment with the standards or regulations. Identity management can be classified into various types, such as centralized, decentralized, or federated.
Centralized identity management is a type of identity management that involves using or applying a single or a central authority or entity, such as a server or a database, to control and manage the identity or the information of the users or the entities, and to provide or grant the access or the authorization to the users or the entities, for accessing or using the system or the network, or the service or the application. Centralized identity management can provide various benefits, such as simplicity, consistency, or scalability.
Centralized identity management can also include various roles or functions, such as:

Credential provider: The role or the function that involves creating and issuing the credentials, such as passwords, tokens, or certificates, to the users or the entities, for authenticating or verifying the identity or the information of the users or the entities, and for accessing or using the system or the network, or the service or the application.
Identity provider (IdP): The role or the function that involves storing and managing the identifiers, such as usernames, email addresses, or phone numbers, and the attributes, such as names, roles, or preferences, of the users or the entities, and providing or sharing the identifiers and the attributes of the users or the entities, with the system or the network, or with the service or the application, for identifying or recognizing the users or the entities, and for accessing or using the system or the network, or the service or the application.
Service provider: The role or the function that involves offering or delivering the system or the network, or the service or the application, to the users or the entities, and requesting or receiving the credentials, the identifiers, or the attributes of the users or the entities, from the credential provider or the identity provider, for authenticating, authorizing, or personalizing the users or the entities, and for accessing or using the system or the network, or the service or the application.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 512
當補丁應用於組織的系統時，下列哪一項最能支援補丁相容性的有效測試？
A. 設備的標準化配置
B. 標準化斑貼測試設備
C. 自動系統修補
D. 修補的管理支持
Answer: A (LEAVE A REPLY)
Standardized configurations for devices can help to reduce the complexity and variability of the systems that need to be patched, and thus facilitate the testing of patch compatibility.
Standardized configurations can also help to ensure that the patches are applied consistently and correctly across the organization. Standardized patch testing equipment, automated system patching, and management support for patching are also important factors for effective patch management, but they are not directly related to testing patch compatibility.

NEW QUESTION: 513
為什麼系統的關鍵性分類對大型組織來口很重要？
A. 它提供了安全和維護任務的合理優先排序和時間安排。

B. 它減少了關鍵系統支援工作量，並減少了應用補丁所需的時間。
C. 它允許向高階管理人員清晰地傳達系統狀態訊息。
D. 它有助於更輕鬆地確定所有權，減少對資口狀態的混淆。
Answer: A (LEAVE A REPLY)
A system's criticality classification is important in large organizations because it provides for proper prioritization and scheduling of security and maintenance tasks. A system's criticality classification is the level of importance or impact that a system has on the organization's mission, objectives, operations, or functions. A system's criticality classification may depend on factors such as the system's availability, integrity, confidentiality, functionality, performance, or reliability.
A system's criticality classification helps the organization to allocate resources, implement controls, perform audits, apply patches, conduct backups, and respond to incidents according to the system's priority and risk. A system's criticality classification does not necessarily reduce critical system support workload or the time required to apply patches, as these may depend on other factors such as the system's complexity, configuration, or vulnerability. A system's criticality classification may allow for clear systems status communications to executive management, but this is not the primary reason for its importance. A system's criticality classification may provide for easier determination of ownership, but this is not the main benefit of its importance.

NEW QUESTION: 514
基於角色的存取控制方法最有效地緩解了哪些安全風險？
A. 對系統和資料擁有過多的存取權限
B. 業務應用程式中的職責分離衝突
C. 缺乏系統管理員活動監控
D. 不當存取請求
Answer: (SHOW ANSWER)
The security risk that the role-based access approach mitigates most effectively is excessive access rights to systems and data. Role-based access control (RBAC) is a model of access control that assigns permissions to roles rather than individual users, and then assigns users to those roles based on their job functions and responsibilities. This way, RBAC ensures that users have the minimum necessary access rights to perform their tasks and reduces the risk of unauthorized or inappropriate access.

NEW QUESTION: 515
應用程式過濾防火牆的一個缺點是它可能導致
A. 由於使用者活動而導致的網路崩潰。
B. 由於應用規則而導致的效能下降。
C. 由於頻寬不足導致網路封包遺失。
D. 駭客對網際網路協定(IP)的欺騙。
Answer: (SHOW ANSWER)

A disadvantage of an application filtering firewall is that it can lead to performance degradation due to the rules applied. An application filtering firewall is a type of firewall that inspects the content and context of the data packets at the application layer of the OSI model. It can block or allow traffic based on the application protocol, the source and destination addresses, the user identity, the time of day, and other criteria. An application filtering firewall provides a high level of security and control, but it also requires more processing power and memory than other types of firewalls. This can result in slower network performance and increased latency.

NEW QUESTION: 516
下列哪一項是異地儲存的主要好處？
A. 成本效益
B. 備份簡單
C. 快速恢復
D. 數據可用性
Answer: D (LEAVE A REPLY)
The main benefit of off-site storage is data availability. Off-site storage is a technique that involves storing backup data or copies of data in a different location than the primary data source, such as a remote data center, a cloud storage service, or a tape vault. Off-site storage can improve data availability, which is the ability to access or use the data when needed, by providing an alternative source of data in case of a disaster or an outage that affects the primary data source. Off-site storage can also protect the data from theft, fire, flood, or other physical threats that may occur at the primary data location.

NEW QUESTION: 517
下列何者最能描述軟體取證的目的？
A. 執行循環冗餘校驗 (CRC) 驗證並偵測更改的應用程式
B. 檢口程式碼以確定是否存在後門
C. 分析惡意軟體可能的惡意意圖
D. 確定程式碼的作者與行為
Answer: D (LEAVE A REPLY)
The best description of the purpose of software forensics is to determine the author and behavior of the code. Software forensics is the application of forensic science to software, which involves the collection, analysis, and presentation of software-related evidence. Software forensics can be used for various purposes, such as investigating software crimes, disputes, or incidents, identifying software vulnerabilities or defects, verifying software compliance or quality, or recovering software data or functionality. However, the primary purpose of software forensics is to determine the author and behavior of the code, which can help to establish the origin, ownership, responsibility, or intention of the software. For example, software forensics can help to identify the creator, distributor, or user of a malware, a pirated software, or a stolen software. Software forensics can also help to understand the functionality, logic, or purpose of a software, such as what it does, how it works, or what it affects. To determine the author and behavior of the code, software forensics can use various techniques, such as

code analysis, code comparison, code reverse engineering, code fingerprinting, or code attribution. To perform cyclic redundancy check (CRC) verification and detect changed applications, to review program code to determine the existence of backdoors, or to analyze possible malicious intent of malware are not the best descriptions of the purpose of software forensics. These are some of the possible applications or outcomes of software forensics, but they are not the main or overarching purpose of software forensics. Moreover, these are not exclusive to software forensics, as they can also be performed by other software-related disciplines, such as software testing, software security, or software engineering.

NEW QUESTION: 518
可以將額外的填充添加到封裝安全協定 (ESP) 尾部以提供下列哪一項？
A. 資料來源認證
B. 部分流量機密性
C. 保護 ao> 免受重播攻擊
D. 存取控制
Answer: B (LEAVE A REPLY)
Additional padding may be added to the Encapsulating Security Protocol (ESP) trailer to provide partial traffic flow confidentiality. ESP is a protocol that provides confidentiality, integrity, and authentication for IP packets. ESP uses encryption to protect the payload of the IP packets, and optionally the IP header as well. ESP also adds a trailer at the end of the IP packet, which contains a padding field, a pad length field, and a next header field. The padding field is used to align the encrypted data to the block size of the encryption algorithm, and to provide partial traffic flow confidentiality by obscuring the actual length of the data. The pad length field indicates the number of bytes in the padding field. The next header field indicates the type of the payload that follows the ESP trailer. Data origin authentication, protection against replay attack, and access control are not provided by the ESP trailer, but by other components of ESP, such as the ESP header, the ESP authentication data, and the security association.

NEW QUESTION: 519
如果由安全資訊和事件管理 (SIEM) 系統報告，下列哪一項將被視為事件？
A. 管理員正在透過虛擬私人網路 (VPN) 登入伺服器。
B. 日誌來源已停止傳送資料。
C. 網路資源報告了 404 錯誤。
D. 防火牆使用連接埠 80 上的傳輸控制協定 (TCP) 記錄 Internet 上的用口端與 Web 伺服器之間的連線。
Answer: B (LEAVE A REPLY)
A log source is a device or system that generates and sends data to a security information and event management (SIEM) system, such as logs, alerts, or events. A log source that has stopped sending data would be considered an incident if reported by a SIEM system, as this could indicate a malfunction, a compromise, or a denial of service attack on the log source. A SIEM system relies on the data from the log sources to provide a comprehensive and accurate view of the security posture and events of the organization. An administrator logging in on a server through a virtual private network

(VPN) would not be considered an incident, as this is a legitimate and authorized activity. A web resource reporting a 404 error would not be considered an incident, as this is a common and benign error that indicates that the requested resource was not found on the server. A firewall logging a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80 would not be considered an incident, as this is a normal and expected traffic for web browsing.

NEW QUESTION: 520
請參考以下資訊回答問題。
安全從業人員偵測到針對組織網路的客口端攻擊。需要製定計劃來應對這些問題。
除了網頁瀏覽器之外，針對用於惡意目的的行動程式碼，還需要重點關注哪些方面？
A. 文字編輯器、資料庫和互聯網電話應用程序
B. 電子郵件、簡報和資料庫應用程式
C. 圖像庫、簡報和電子表格應用程式
D. 電子郵件、媒體播放器和即時通訊應用程式
Answer: D (LEAVE A REPLY)
The primary areas that need to be addressed concerning mobile code used for malicious purposes, in addition to web browsers, are email, media players, and instant messaging applications. Mobile code is a type of code that can be transferred or executed over a network, such as the internet, without the user's knowledge or consent, and that can perform various functions or tasks on the user's system, such as displaying advertisements, collecting information, or installing malware. Mobile code can be embedded or attached in various types of applications or files, such as web browsers, email, media players, or instant messaging applications, and can pose a serious security threat to the user's system or data. Text editors, database, and internet phone applications are not the primary areas that need to be addressed concerning mobile code used for malicious purposes, as they are not the common or likely sources or targets of the mobile code attacks, and they may not support or execute the mobile code as easily or frequently as the other applications.

NEW QUESTION: 521
分析可執行檔時靜態分析的目的是什麼？
A. 收集可執行檔的使用證據，包括建立日期和上次使用日期。
B. 搜尋與執行檔關聯的文件和文件。
C. 分析檔案在檔案系統中的位置以及可執行檔案的函式庫。
D. 反組譯文件以收集有關執行檔功能的資訊。
Answer: D (LEAVE A REPLY)
Static analysis is a technique of examining the code or structure of a file or program without executing it. Static analysis can be used to identify potential vulnerabilities, errors, or malicious code in a file or program. One of the methods of static analysis is disassembly, which is the process of converting the binary code of an executable file into a human-readable assembly language. Disassembly can reveal information about the executable file's function, such as the instructions, variables, registers, memory

addresses, and system calls. Disassembly can also help to reverse engineer the logic and algorithm of the executable file. Collecting evidence of the executable file's usage, such as dates of creation and last use, is not the purpose of static analysis, but rather a forensic analysis technique. Searching the documents and files associated with the executable file is not a static analysis technique, but rather a data discovery or classification technique. Analyzing the position of the file in the file system and the executable file's libraries is not a static analysis technique, but rather a dependency analysis or configuration management technique.

NEW QUESTION: 522
以下哪□最能描述“气隙式”系□？
A. □接到互□网但受到□大防火□保□的系□
B. 与包括互□网在内的不安全网□物理隔离、无直接网□□接的系□，用于保□高度敏感或关□系□免受□程网□攻□。
C. □使用无□□接□行所有通信的系□
D. 用于描述具有冗余□源的系□的一个□□
Answer: B (LEAVE A REPLY)
Air-gapped systems are physically isolated from unsecured networks, including the internet and other internal networks, with no direct network connectivity whatsoever, providing a high level of protection against remote, network-based attacks for highly sensitive or critical systems (such as certain industrial control systems or classified government systems), though they remain vulnerable to other vectors such as removable media or insider threats.

NEW QUESTION: 523
對屬於同一組織的設備進行相互身份驗證的最佳方式是什麼？
A. 令牌
B. 證書
C. 使用者 ID 和密碼
D. 生物識別
Answer: (SHOW ANSWER)
Certificates are the best way for mutual authentication of devices belonging to the same organization. Mutual authentication is a process that involves verifying the identity and the legitimacy of both parties involved in a communication or a transaction, and ensuring that they are authorized and trusted to access or exchange the information or the resources. Certificates are the digital documents that contain the identity and the public key of a device, a user, or an entity, and that are issued and signed by a trusted authority, such as a Certificate Authority (CA).
Certificates can be used for mutual authentication of devices belonging to the same organization, as they can provide a secure and reliable way of verifying and exchanging the public keys of the devices, and of encrypting and decrypting the data or the messages that are transmitted between the devices. Certificates can also prevent or detect various attacks or threats that may compromise the mutual authentication of the devices, such as impersonation, spoofing, replay, or man-in-the-middle attacks. Therefore, certificates are the best way for mutual authentication of devices belonging to the same

organization, as they can ensure the confidentiality, the integrity, and the authenticity of the communication or the transaction between the devices.

NEW QUESTION: 524
下列哪一項是最常見的記憶體保護方法？
A. 劃分
B. 分段
C. 糾錯
D. 虛擬區域網路 (VLAN) 標記
Answer: B (LEAVE A REPLY)
The most common method of memory protection is segmentation. Segmentation is a technique that divides the memory space into logical segments, such as code, data, stack, and heap. Each segment has its own attributes, such as size, location, access rights, and protection level.
Segmentation can help to isolate and protect the memory segments from unauthorized or unintended access, modification, or execution, as well as to prevent memory corruption, overflow, or leakage. Compartmentalization, error correction, and VLAN tagging are not methods of memory protection, but of information protection, data protection, and network protection, respectively.

NEW QUESTION: 525
以下哪□最能描述“出□点零知□□明”的目的？
A. 一种要求一方□□明其主□而向另一方完全披露其秘密信息的方法
B. 一种加密方法，允□一方向另一方□明特定□述□真，而无需泄露除□述本身有效性之外的任何其他信息。
C. 一种□□大型加密密□的技□
D. 一种□□用于网□路由的□□
Answer: (SHOW ANSWER)
A zero-knowledge proof is a cryptographic technique that allows one party (the prover) to convince another party (the verifier) that a specific statement is true-such as knowing a secret password or having sufficient funds for a transaction-without revealing any information about the underlying secret itself beyond the fact that the statement is valid.

NEW QUESTION: 526
在滲透測試期間，規劃階段的三個主要目標是什麼？
A. 確定測試目標、確定參與規則並進行初步發現掃描。
B. 完成管理階層批准、確定測試目標並收集連接埠和服務資訊。
C. 確定參與規則、最終確定管理階層批准並確定測試目標。
D. 確定參與規則、文件管理審批，並收集系統和應用程式資訊。
Answer: C (LEAVE A REPLY)

The three primary objectives of the planning phase of a penetration test are to identify the rules of engagement, finalize the management approval, and determine the testing goals. The rules of engagement define the scope, boundaries, methods, and communication channels of the test. The management approval ensures the legal and ethical authorization of the test. The testing goals specify the desired outcomes and deliverables of the test.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 527
以下哪個術語用於在聯盟口運營的線上服務提供者？
A. Active Directory 聯合身分驗證服務 (ADFS)
B. 依賴方 (RP)
C. 單一登入 (SSO)
D. 身分與存取管理 (IAM)
Answer: A (LEAVE A REPLY)
In a federated identity system, the relying party (RP) is a service provider that relies on an identity provider (IdP) to authenticate and provide identity information for users. This allows users to access multiple services using a single sign-on (SSO) across different providers while maintaining their identity and access management (IAM) across these services.

NEW QUESTION: 528
軟體安全功能需求必須在軟體開發生命週期(SDLC)的哪個階段定義？
A. 在系統初步設計完成後，並進行資料安全分類後
B. 在完成漏洞分析後，在系統詳細設計開始前
C. 在系統初步設計完成後、資料安全分類開始前
D. 在完成業務功能分析和資料安全分類後
Answer: D (LEAVE A REPLY)
Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed in the Software Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:

System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and establishing the project plan and budget.
System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.
System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.
System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.
Software security functional requirements are the specific and measurable security features and capabilities that the system must provide to meet the security objectives and requirements.
Software security functional requirements are derived from the business functional analysis and the data security categorization, which are two tasks that are performed in the system initiation phase of the SDLC. The business functional analysis is the process of identifying and documenting the business functions and processes that the system must support and enable, such as the inputs, outputs, workflows, and tasks. The data security categorization is the process of determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures. Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed, because they can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system security is aligned and integrated with the business functions and processes.

NEW QUESTION: 529
以下哪种□□控制模型基于□求□□估的用□、□源和□境属性的□合来授予或拒□□□□限？
A. 自主□□控制(DAC)
B. 基于□□的□□控制
C. 基于属性的□□控制(ABAC)
D. □制□□控制(MAC)
Answer: (SHOW ANSWER)
ABAC evaluates a combination of attributes-such as user role, department, resource sensitivity, time of day, and location-against policy rules at the time of the access request, providing fine- grained, context-aware access decisions beyond static role or label assignments.

NEW QUESTION: 530
關於□邊界分析作為一種功能性軟體測試技術，下列哪一個敘述是正確的？

A. 它可用於測試通訊協定和圖形使用者介面。
B. 它的特徵是函數中實現的程序的無狀態行為。
C. 測試輸入是從給定功能規範的導出閾□中獲得的。
D. 只需考慮分割區中的一個代表□即可覆寫整個分割區。
Answer: C (LEAVE A REPLY)
Value boundary analysis is a functional software testing technique that tests the behavior of a software system or component when it receives inputs that are at the boundary or edge of the expected range of values. Value boundary analysis is based on the assumption that errors are more likely to occur at the boundary values than at the normal values. Test inputs are obtained from the derived threshold of the given functional specifications, such as the minimum, maximum, or just above or below the boundary values. Value boundary analysis can help identify errors or defects in the software system or component that may cause unexpected or incorrect outputs, crashes, or failures

NEW QUESTION: 531
以下哪□最能描述"□□□□性□划：恢复策略□□□准?
A. 不考□□□需求，□□成本最低的恢复策略
B. 根据□□功能的关□性(由□□影响分析 (BIA) 提供信息)、可接受的恢复□□目□ (RTO)/恢复点目□ (RPO) 以及恢复解决方案的成本相□于停机□□潜在影响的平衡来□□恢复策略。
C. □根据□工意愿□□恢复策略
D. □所有□□功能□□□一的、通用的恢复策略，而不考□其关□性
Answer: B (LEAVE A REPLY)
Recovery strategy selection should be informed by the results of the Business Impact Analysis, balancing the criticality of each business function, its acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and the cost of implementing a given recovery solution relative to the potential financial and operational impact of extended downtime-ensuring that resources are allocated proportionally to the most critical functions rather than uniformly across all systems.

NEW QUESTION: 532
下列哪一項是在使用卡片存取的設施的入口點僱用實體安全人員的主要原因？
A. 驗證只有員工有權存取該設施。
B. 辨識目前需要補救的危險。
C. 監控整個設施□的員工活動。
D. 提供員工安全的環境。
Answer: D (LEAVE A REPLY)
Security personnel contribute to the overall safety and security of the facility and its employees, particularly in emergency situations, and act as a deterrent to potential threats.

NEW QUESTION: 533
在測試環境中匿名化個人識別資訊 (PII) 的最佳方法是什麼？
A. 隨機化數據

B. 交換數據
C. 加密數據
D. 編碼數據
Answer: A (LEAVE A REPLY)
The best approach to anonymizing personally identifiable information (PII) in a test environment is randomizing data. Randomizing data is a technique that replaces the original PII with fictitious but realistic data that preserves the format, structure, and statistical properties of the original data. Randomizing data can effectively protect the privacy and confidentiality of the individuals whose PII is used in the test environment, while maintaining the functionality and quality of the test results.

NEW QUESTION: 534
點對點協定（PPP）是專門為了解決什麼問題而設計的？
A. 電話數據機的常見設計缺陷
B. 撥接使用者和 Internet 服務供應商 (ISP) 之間的速度和可靠性問題
C. 個人電腦和網頁瀏覽器的相容性問題
D. 遠端網路撥號連線的安全性
Answer: D (LEAVE A REPLY)
Point-to-Point Protocol (PPP) is a network protocol that provides a simple and secure way of establishing a direct connection between two hosts over a serial link, such as a phone line or a cable. PPP was designed to specifically address the issue of the security of dial-up connections to remote networks. A dial-up connection is a type of connection that uses a phone line and a modem to connect to a remote network, such as the internet or a corporate network. A dial-up connection is often insecure and vulnerable to various threats, such as eavesdropping, spoofing, or hijacking. PPP was designed to enhance the security of dial-up connections by supporting various features, such as authentication, encryption, compression, error detection, and negotiation. Authentication is the process of verifying the identity and credential of the hosts or users involved in the connection. Encryption is the process of transforming the data into an unreadable form to prevent unauthorized access or disclosure of the data. Compression is the process of reducing the size of the data transmitted over the network to improve the performance and efficiency of the connection. Error detection is the process of identifying and correcting any errors or faults that may occur during the transmission. Negotiation is the process of agreeing on the parameters, options, and features of the connection between the hosts. PPP can help to protect the dial-up connections from various threats by using these features, as well as by using various protocols, such as Link Control Protocol (LCP) or Network Control Protocol (NCP). A common design flaw in telephone modems, speed and reliability issues between dial-up users and Internet Service Providers (ISP), or compatibility issues with personal computers and web browsers are not the issues that PPP was designed to specifically address, as they are more related to the hardware, network, or software aspects of dial-up connections.

NEW QUESTION: 535
以下哪□最能描述“不可否□性”的概念？
A. 保□一方不能否□已□行特定行□，例如□送消息或授□交易。

B. 保□数据未泄露□未□授□的各方
C. 确保系□在高峰需求期□仍能保持可用
D. 确保数据的准确性和完整性
Answer: A (LEAVE A REPLY)
Non-repudiation provides assurance that a party cannot later deny having performed a specific action, such as sending a message, approving a transaction, or accessing a system, typically achieved through mechanisms like digital signatures, audit logs, and timestamps that create verifiable evidence of the action.

NEW QUESTION: 536
請參考以下資訊回答問題。
遭受財務衝擊的組織被迫削減預算，並減少負責基本邏輯存取安全管理職能的資訊科技IT)維運人員數量。安全流程已與常規IT運作緊密整合，並非獨立且不同的職能。
當員工離開組織時，下列哪一項將是首要的安全問題？
A. IT支援不足
B. 資料遺失與職責分離
C. 未記錄的安全控制
D. 剩餘員工的額外職責
Answer: B (LEAVE A REPLY)
The primary security concern as staff is released from the organization is the loss of data and separation of duties. The loss of data is the event or the situation where the data is deleted, corrupted, stolen, or leaked by the staff who are leaving the organization, either intentionally or unintentionally, and where the data is no longer available or recoverable by the organization. The loss of data can compromise the confidentiality, the integrity, and the availability of the data, and can cause damage or harm to the organization's operations, reputation, or objectives. The separation of duties is the principle or the practice of dividing the tasks or the responsibilities among different staff or roles, to prevent or reduce the conflicts of interest, the collusion, the fraud, or the errors. The separation of duties can be compromised when the staff is released from the organization, as it can create the gaps or the overlaps in the tasks or the responsibilities, and it can increase the risk of the unauthorized or the malicious access or activity. Inadequate IT support, undocumented security controls, and additional responsibilities for remaining staff are not the primary security concerns as staff is released from the organization, as they are related to the quality, the transparency, or the workload of the IT operations, not the loss of data or the separation of duties.

NEW QUESTION: 537
以下哪□最能描述“出口点行□生物□□”作□一种持□身份□□技□的用途？
A. □在首次登□□□行的一次性指□□描
B. 持□分析用□在整个会□期□的独特行□模式(例如打字□奏、鼠□移□或触摸屏手□)，以□□已□□用□是否□同一人，从而□□□□□□盗用或会□劫持。
C. 一种静□生物特征数据加密方法

D. 一种□□用于物理□禁控制的技□

Answer: B (LEAVE A REPLY)

Behavioral biometrics continuously analyzes unique, largely unconscious patterns in how a user interacts with a system-such as typing rhythm/cadence, mouse movement patterns, or touchscreen gesture dynamics-throughout an active session, rather than relying solely on a one- time authentication event at login. This enables continuous, passive verification that the currently active user remains the same legitimately authenticated individual, potentially detecting account takeover, session hijacking, or credential sharing in real time.

NEW QUESTION: 538

在考慮業務連續性 (BC) 和災難復原 (DR) 培訓計劃的有效性時，最重要的因素是什麼？

A. 管理支持

B. 考慮組織需求

C. 用於交付的技術

D. 目標受眾

Answer: A (LEAVE A REPLY)

The effectiveness of a BC/DR training program largely depends on management support because it ensures adequate resources, prioritization, and enforcement of policies are in place to make the training effective across the organization.

NEW QUESTION: 539

管理層已決定將核心應用程式用於個人蜂窩電話。作為實施要求，需要定期對安全態勢進行分析 管理階層也指示實施持續監控。為了完成管理階層的指示，需要下列哪一項？

A. 應用程式管理、設定管理（CM）和電話管理的嚴格集成

B. 安裝在用□手機上的管理應用程序，用於追蹤所有應用程式事件和蜂窩流量

C. 企業級安全資訊和事件管理 (SIEM) 儀表板，提供手機活動的完整可見性

D. 由使用者的行動電話提供者□生的詳細□明安全事件的例行報告

Answer: (SHOW ANSWER)

When a core application runs on personal cellular phones, continuous monitoring and regular security-posture analysis require a coordinated framework across:

Application management (how the app is deployed, updated, and secured).

Configuration management (CM) (ensuring devices and app settings comply with security baselines).

Phone management (via a mobile device management [MDM] or unified endpoint management [UEM] platform that can enforce policies, detect anomalies, and respond to incidents).

Only tight integration of these three areas can provide the regular analysis and continuous monitoring that management has directed.

NEW QUESTION: 540

一個組織最近對其網路應用程式的安全性進行了審□。發現的漏洞之一是用於向第三方伺服器加密敏感資訊的會話金鑰已被硬編碼在客□端和伺服器應用程式中。下列哪一項對於緩解此漏洞最有效？

A. Diffle-Hellman (DH) 演算法
B. 橢圓曲線加密 (ECC) 演算法
C. 數位簽章演算法 (DSA)
D. Rivest-Shamir-Adleman (RSA) 演算法
Answer: (SHOW ANSWER)
The vulnerability described in the question relates to a hard-coded session key in both the client and server applications, which is a security risk. Hard-coding cryptographic keys in source code exposes them to potential attackers who could extract them through reverse engineering or other means.
The Diffie-Hellman (DH) algorithm is the most effective way to mitigate this vulnerability. DH is a key exchange algorithm that allows two parties (the client and the server) to securely establish a shared session key over an insecure channel, without ever transmitting the key itself. This means that, instead of hard-coding a session key, the client and server can use DH to dynamically generate the session key during the connection establishment, which is much more secure.
Once the session key is generated via DH, it can be used for encrypting the communication between the client and server, and because the key is not hard-coded, it eliminates the vulnerability of key exposure.

NEW QUESTION: 541
以下哪□最能描述“运行□□用程序自我保□(RASP)”的目的？
A. 一种在部署前□描源代□漏洞的工具
B. 一种嵌入在□用程序内部或与□用程序在运行□□接的安全技□，能□根据□用程序的□□行□和上下文□□□□和阻止攻□。
C. 一种基于网□的防火□，用于□□网□□界的流量
D. 一种□□用于□□均衡□用程序流量的工具
Answer: B (LEAVE A REPLY)
RASP is a security technology integrated directly within or alongside a running application, monitoring its behavior and execution context in real time to detect and block attacks (such as injection attempts) as they occur, leveraging the application's internal visibility to provide more precise, context-aware protection than external network-based controls like a traditional WAF.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 542
一家公司希望在異地伺服器上儲存與用□相關的資料。可以採用什麼方法來保護使用者資訊的隱私，同時維護資料庫的欄位層級配置？

A. 加密
B. 編碼
C. 標記化
D. 雜湊
Answer: C (LEAVE A REPLY)
The method that can be deployed to protect the privacy of the user's information while maintaining the field-level configuration of the database is tokenization. Tokenization is a technique that replaces sensitive data, such as personal or financial information, with nonsensitive placeholders, called tokens. Tokens are randomly generated values that have no intrinsic meaning or value, and cannot be reversed or decrypted to reveal the original data.
Tokens can preserve the format, length, and type of the original data, and can be stored in the same database fields as the original data. Tokenization can protect the privacy of the user's information by reducing the exposure and risk of data breaches, as the tokens are useless for the attackers who may access the database. Tokenization can also maintain the field-level configuration of the database, as the tokens can be used for the same purposes as the original data, such as processing, analysis, or reporting, without affecting the database structure or functionality.

NEW QUESTION: 543
請參考以下資訊回答問題。
在多層安全 (MLS) 系統中，敏感度標籤會依敏感度遞增的順序排列如下：限制等級機密等級、秘密等級、口密級。表 A 列出了四位使用者的安全級別，表B 列出了四個不同文件的安全等級。

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

在 Bell-LaPadula 系統中，哪個使用者在向四個檔案中的任何一個寫入資料時受到的限制最多？
A. 使用者 A
B. 使用者 B
C. 使用者 C
D. 使用者 D
Answer: A (LEAVE A REPLY)
In a Bell-LaPadula system, a user has the most restrictions when writing data to any of the four files if they have the lowest clearance level. This is because of the star property (*property) of the Bell-LaPadula model, which states that a subject with a given security clearance may write data to an object if and only if the object's security level is greater than or equal to the subject's security level. This rule is also known as the no write-down rule, as it prevents the leakage of information from a higher level to a lower level. In this question, User A has a Restricted clearance, which is the lowest level among the four users. Therefore, User A has the most restrictions when writing data to any of the four files, as they can only write data to File 1, which has the same security level as their clearance. User B, User C, and

User D have less restrictions when writing data to any of the four files, as they can write data to more than one file, depending on their clearance levels and the security classes of the files.

NEW QUESTION: 544
如何才能最好地利用從業務連續性培訓和實際恢復事件中學到的經驗教訓？
A. 作為一種改進手段
B. 作為提高意識和培訓的替代方案
C. 作為政策需求的指標
D. 作為業務功能差距指標
Answer: A (LEAVE A REPLY)
The best way to use the lessons learned from business continuity training and actual recovery incidents is as a means for improvement. Business continuity training is a process or a technique that educates or trains the personnel or the staff of the organization, such as the employees, the contractors, or the partners, on the business continuity plan or the document that defines or specifies the procedures or the actions that are performed or executed by the organization, such as the business, the enterprise, or the institution, to continue or to resume the critical or the essential functions or operations of the organization, such as the services, the products, or the processes, after or during the occurrence or the happening of the disaster or the event that causes or results in the disruption, the interruption, or the damage of the functions or operations of the organization, such as the fire, the flood, or the cyberattack. Actual recovery incidents are the scenarios or the situations that occur or happen in the real world or the reality, where the organization, such as the business, the enterprise, or the institution, experiences or faces the disaster or the event that causes or results in the disruption, the interruption, or the damage of the functions or operations of the organization, such as the fire, the flood, or the cyberattack, and where the organization implements or applies the business continuity plan or the document that defines or specifies the procedures or the actions that are performed or executed by the organization, to continue or to resume the critical or the essential functions or operations of the organization, such as the services, the products, or the processes. Lessons learned are the outcomes or the results of the business continuity training and the actual recovery incidents, that provide or offer the feedback, the evaluation, or the assessment of the effectiveness or the efficiency of the business continuity plan, and that identify or detect the strengths, the weaknesses, the opportunities, or the threats of the business continuity plan. The best way to use the lessons learned from business continuity training and actual recovery incidents is as a means for improvement, which means that the lessons learned from business continuity training and actual recovery incidents are used or applied to improve or enhance the business continuity plan, by addressing or resolving the issues, the gaps, or the problems of the business continuity plan, by incorporating or integrating the best practices, the standards, or the guidelines of the business continuity plan, and by updating or maintaining the business continuity plan to reflect or represent the current or the accurate needs, the requirements, or the expectations of the organization, such as the business, the enterprise, or the institution.

NEW QUESTION: 545

一個大型人力資源組織希望將其身分管理與口得信賴的合作夥伴組織整合。人力資源組織希望維持身分的創建和管理，並可能希望在未來與其他合作夥伴分享。下列哪一個選項最能滿足他們的需求？
A. 聯合身份
B. 雲端 Active Directory (AD)
C. 安全性斷言標記語言 (SAML)
D. 單一登入 (SSO)
Answer: A (LEAVE A REPLY)
Federated identity is a mechanism that allows users to use a single identity across multiple systems or organizations, without requiring the creation or management of separate accounts for each system or organization. Federated identity relies on trust relationships between the identity providers (IdPs) and the service providers (SPs) that participate in the federation. The IdPs are responsible for authenticating the users and issuing security tokens that contain identity attributes or claims. The SPs are responsible for validating the security tokens and granting access to the users based on the identity attributes or claims. Federated identity enables users to have a seamless and consistent user experience, while reducing the administrative overhead and security risks associated with multiple accounts. Federated identity also supports the principle of data minimization, as the IdPs only share the necessary identity attributes or claims with the SPs, and the SPs do not store any user identity information. Federated identity is often implemented using standards such as Security Assertion Markup Language (SAML), OpenID Connect, or OAuth.

NEW QUESTION: 546
應用下列哪一項標準最能減少資料外洩的可能性？
A. ISO 9000
B. ISO 20121
C. ISO 26000
D. ISO 27001
Answer: (SHOW ANSWER)
The standard that would best reduce the potential for data breaches is ISO 27001. ISO 27001 is an international standard that specifies the requirements and the guidelines for establishing, implementing, maintaining, and improving an information security management system (ISMS) within an organization. An ISMS is a systematic approach to managing the information security of the organization, by applying the principles of plan-do-check-act (PDCA) cycle, and by following the best practices of risk assessment, risk treatment, security controls, monitoring, review, and improvement. ISO 27001 can help reduce the potential for data breaches, as it can provide a framework and a methodology for the organization to identify, protect, detect, respond, and recover from the information security incidents or events that could compromise the confidentiality, integrity, or availability of the data or the information.

NEW QUESTION: 547
在保護系統、應用程式和委託資訊的價口同時避免利益衝突時，最能體現哪一條(ISC) 道德準則？
A. 行事誠實、誠實、公正、負責且合法。

B. 保護社會、聯邦和基礎設施。
C. 為原則提供勤奮和稱職的服務。
D. 促進和保護職業。
Answer: C (LEAVE A REPLY)
Under the third canon, provide diligent and competent service to principals,?they offer this guidance:
Preserve the value of their systems, applications and information.
Respect their trust and the privileges that they grant you.
Avoid conflicts of interest or the appearance thereof.
Render only those services for which you are fully competent and qualified.

NEW QUESTION: 548
以下哪□最能描述“凭□填充”攻□？
A. 攻□者□□所有可能的字符□合来猜□□个密□
B. 攻□者利用先前泄露的用□名/密□□列表(□些列表来自其他无关的数据泄露事件)，自□□□登□多个不同的网站，利用密□重复使用漏洞。
C. 攻□者利用 SQL 注入漏洞从数据□中提取凭据
D. 攻□者□眼目睹用□□入凭据。
Answer: (SHOW ANSWER)
Credential stuffing attacks use large lists of username/password pairs obtained from previous, often unrelated data breaches, and automatically attempt to use them to log into other websites and services, exploiting the common practice of password reuse across multiple accounts-distinct from brute-force attacks, which attempt many password guesses against a single account without prior knowledge of valid credentials.

NEW QUESTION: 549
依賴安全□容自動化協定 (SCAP) 的主要好處是什麼？
A. 為組織節省安全成本。
B. 提高漏洞評估能力。
C. 標準化軟體安全□品之間的規格。
D. 實現組織符合國際標準。
Answer: (SHOW ANSWER)
The primary benefit of relying on Security Content Automation Protocol (SCAP) is to standardize specifications between software security products. SCAP is a suite of specifications that enable the automated and interoperable assessment, measurement, and reporting of the security posture and compliance of systems and networks. SCAP consists of six components: Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Extensible Configuration Checklist Description Format (XCCDF), and Open Vulnerability and Assessment Language (OVAL). SCAP enables different software security products, such as scanners, analyzers, or auditors, to use a

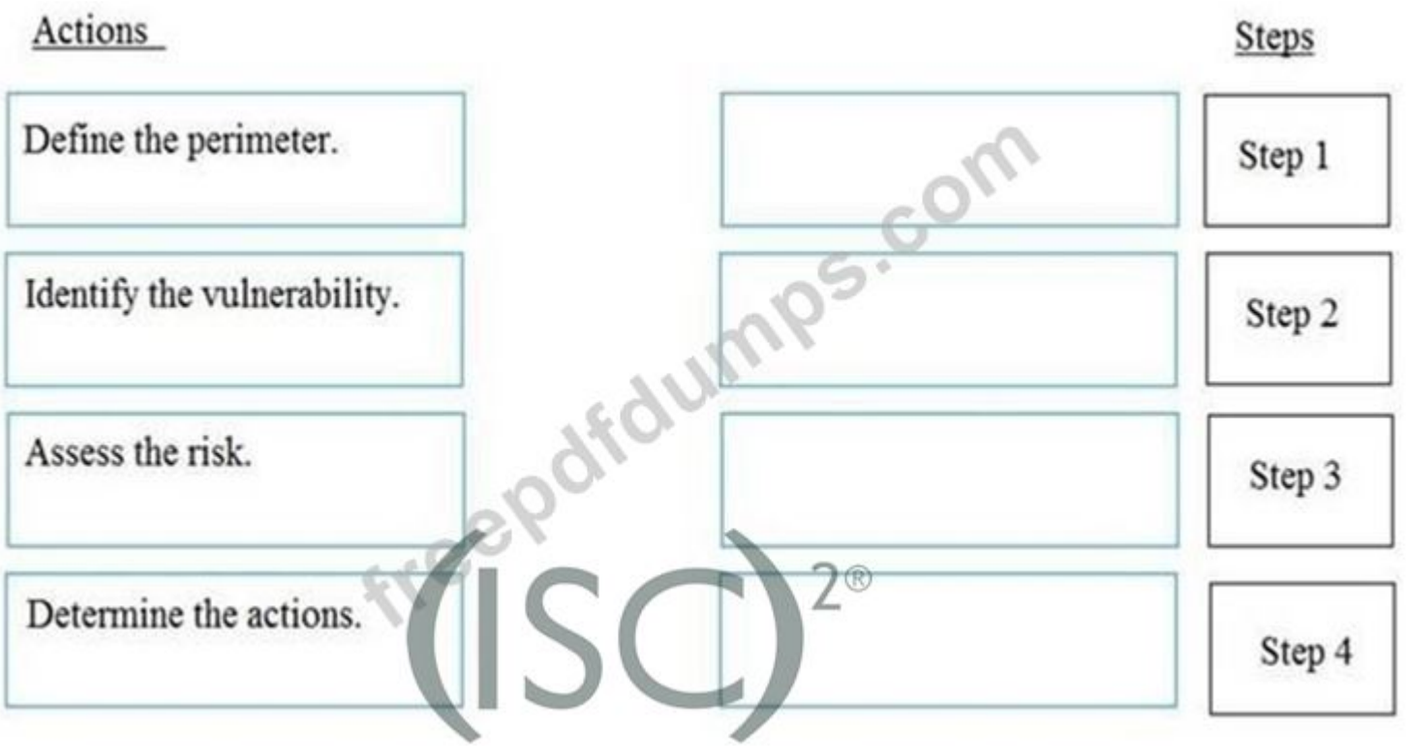
common language and format to describe and exchange information about the security configuration, vulnerabilities, and risks of systems and networks.
This can improve the accuracy, consistency, and efficiency of the security assessment and remediation processes, and reduce the complexity and cost of managing multiple security products. Saving security costs for the organization, improving vulnerability assessment capabilities, and achieving organizational compliance with international standards are also benefits of relying on SCAP, but they are not the primary benefit. Saving security costs for the organization is a benefit of relying on SCAP, as it can reduce the need for manual and labor- intensive security tasks, and increase the reuse and integration of security data and tools.
Improving vulnerability assessment capabilities is a benefit of relying on SCAP, as it can provide more comprehensive, timely, and reliable information about the security weaknesses and exposures of systems and networks, and enable more effective and proactive mitigation and response actions.
Achieving organizational compliance with international standards is a benefit of relying on SCAP, as it can help to demonstrate and verify the alignment of the security policies and practices of the organization with the established benchmarks and baselines, such as the National Institute of Standards and Technology (NIST) Special Publication 800-53 or the International Organization for Standardization (ISO) 27001.

NEW QUESTION: 550
下列哪一項是及時安裝軟體修補程式最重要的原因？
A. 攻擊者可能正在進行網路分析。
B. 補丁僅在特定時間可用。
C. 攻擊者對修補程式中的漏洞進行逆向工程。
D. 補丁可能與專有軟體不相容
Answer: C (LEAVE A REPLY)
The most important reason for timely installation of software patches is that attackers reverse engineer the exploit from the patch. A software patch is a piece of code that is applied to a software program or system to fix a bug, a vulnerability, or a performance issue. A software patch can improve the functionality, security, and stability of the software or system. An exploit is a piece of code or a technique that takes advantage of a vulnerability to compromise or damage a software program or system. An exploit can cause unauthorized access, data loss, denial of service, or malicious code execution. Attackers reverse engineer the exploit from the patch, meaning that they analyze the patch to understand what vulnerability it fixes, and then create or modify an exploit to target that vulnerability. Attackers can use the exploit to attack the software or system that has not been patched yet, or that has been patched but not properly configured or tested. Therefore, timely installation of software patches is crucial to prevent or mitigate the attacks that exploit the known vulnerabilities. Attackers may be conducting network analysis, patches are only available for a specific time, and patches may not be compatible with proprietary software are not as important reasons for timely installation of software patches, as they may not pose as much threat or impact as attackers reverse engineering the exploit from the patch, or they may not be true or relevant in all cases.

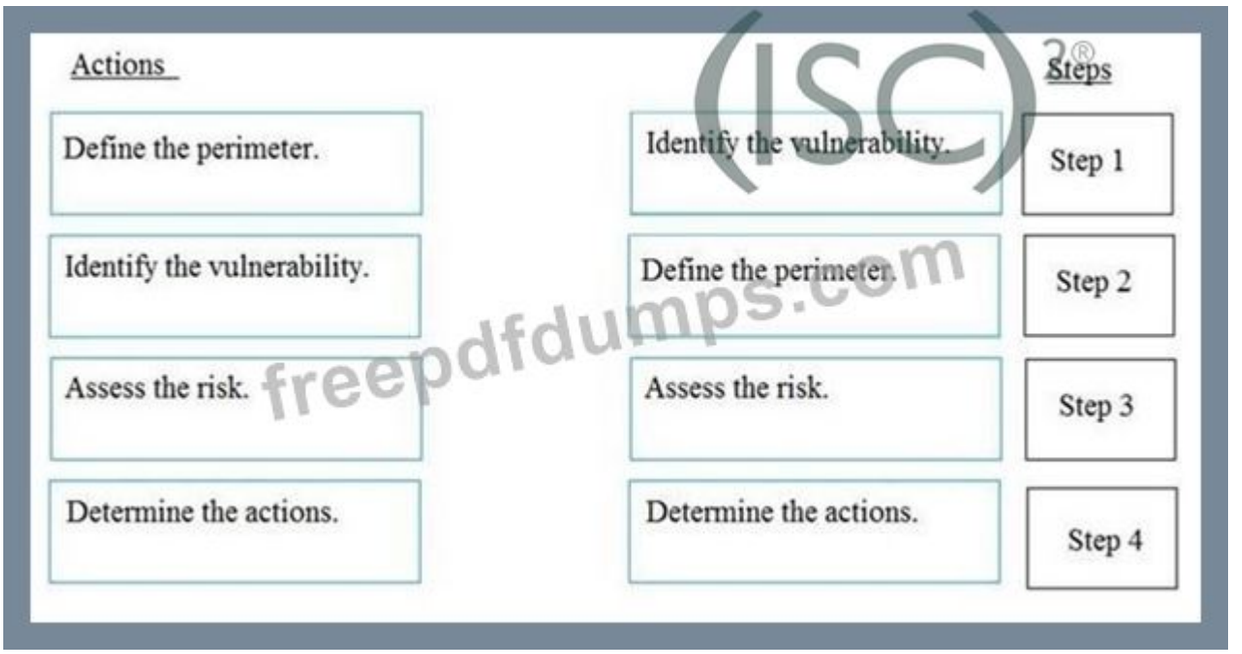
NEW QUESTION: 551
一家大公司正在尋找一種解決方案，根據請求的來源 用口是誰、他們連接的設備以及他們嘗試訪問的時間來自動進行存取。什麼類型的解決方案適合他們的需求？
A. 自主存取控制 (DAC)
B. 基於角色的存取控制 (RBAC)
C. 強制存取控制 (MAC)
D. 網路存取控制 (NAC)
Answer: (SHOW ANSWER)
The type of solution that would suit the needs of a large corporation that wants to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what time of day they are attempting this access is Network Access Control (NAC). NAC is a solution that enables the enforcement of security policies and rules on the network level, by controlling the access of devices and users to the network resources. NAC can automate access based on various factors, such as the location, identity, role, device type, device health, or time of the request. NAC can also perform functions such as authentication, authorization, auditing, remediation, or quarantine of the devices and users that attempt to access the network. Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Mandatory Access Control (MAC) are not types of solutions, but types of access control models that define how the access rights or permissions are granted or denied to the subjects or objects.

NEW QUESTION: 552
安全策略和安全程序的主要區別是什麼？
A. 政策用於強制執行違規行為，程序用於制定處罰措施。
B. 政策指向指導方針，而程序則更具契約性質。
C. 政策包含在意識訓練中，程序提供指導。
D. 政策本質上是通用的，而程序包含操作細節。
Answer: D (LEAVE A REPLY)
The primary difference between security policies and security procedures is that policies are generic in nature, and procedures contain operational details. Security policies are the high-level statements or rules that define the goals, objectives, and requirements of security for an organization. Security procedures are the low-level steps or actions that specify how to implement, enforce, and comply with the security policies.

NEW QUESTION: 553
拖放問題
資訊安全評估的正確步驟順序是什麼？
依照正確的順序將資訊安全評估步驟放在右側編號框旁的左側。



Answer:



NEW QUESTION: 554

外部攻擊者已攻破組織的網路安全邊界，並在口部電腦上安裝了嗅探器。下列哪一項是該組織可以實施的最有效的安全措施，以降低攻擊者獲取更多資訊的可能性？

A. 在網路防火牆上實施封包過濾

B. 請管理員進行強式驗證

C. 安裝基於主機的入侵偵測系統(HIDS)

D. 在交換器上實現邏輯網路分段。

Answer: D (LEAVE A REPLY)

The most effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information is to implement logical network segmentation at the switches. Logical network segmentation is the process of dividing a network into smaller subnetworks or segments based on criteria such as function, role, or access level. This way, the organization can isolate the traffic and data of different segments, and limit the exposure and impact of an attack. If the attacker has installed a sniffer onto an inside computer, logical network segmentation can prevent the sniffer from capturing the traffic and data of other segments, thus reducing the information leakage.

NEW QUESTION: 555
基於角色的存取控制(RBAC)的一個重要特點是什麼？
A. 支援強制存取控制(MAC)
B. 簡化存取權限管理
C. 靠輪崗
D. 需要雙重認證
Answer: B (LEAVE A REPLY)
An important characteristic of Role Based Access Control (RBAC) is that it simplifies the management of access rights. RBAC is a model of access control that assigns permissions to roles, rather than individual users. Users are then assigned to roles based on their job functions or responsibilities. RBAC simplifies the management of access rights by reducing the complexity and overhead of granting, revoking, or modifying permissions for each user. RBAC also improves the consistency and security of access control by enforcing the principle of least privilege and separation of duties.

NEW QUESTION: 556
新站點的閘道無法與總部現有的站點到站點 Internet 協定安全性 (IPsec) 虛擬私人網路 (VPN) 裝置形成隧道。新站點的裝置存取 Internet 上的資源沒有問題。在測試遠端站點閘道之間的連線時，發現網關的外部 Internet 協定 (IP) 位址設定為 192.168.1.1。並配置為將出站流量傳送至 Internet 服務供應商 (ISP) 閘道 at4 192.168.1.2。下列哪一項是解決問題並連接遠端站點的最佳方法？
A. 在新站點和公司總部的VPN設備上口用IPSec隧道模式。
B. 在新站點和公司總部的 VPN 設備上口用第 2 層隧道協定 (L2TP)。
C. 在新站點和公司總部的 VPN 設備上口用點對點隧道協定 (PPTP)。
D. 口用網路位址轉換 (NAT) - 在新站點和公司總部的 VPN 裝置上進行遍歷。
Answer: (SHOW ANSWER)
The best way to resolve the issue and get the remote site connected is to enable NAT-Traversal on the VPN devices at the new site and the corporate headquarters. NAT-Traversal is a technique that allows IPsec VPN devices to operate behind a NAT device, such as a router or a firewall, and establish a tunnel with another IPsec VPN device on the internet. NAT-Traversal encapsulates the IPsec packets in User Datagram Protocol (UDP) packets, and uses a special port (4500) to bypass the NAT device and reach the destination IPsec VPN device. NAT- Traversal solves the problem of IP address mismatch, as it allows the IPsec VPN devices to use their private IP addresses, rather than their public IP addresses, to communicate with each other.

In this scenario, the new site's gateway has a private IP address (192.168.1.1) that is not routable on the internet, and the ISP gateway performs NAT to translate the private IP address to a public IP address. However, this causes the IPsec VPN device at the headquarters to reject the connection request from the new site's gateway, as it expects the public IP address of the new site's gateway to match the private IP address in the IPsec packet. By enabling NAT-Traversal on both VPN devices, the new site's gateway can use its private IP address to form a tunnel with the headquarters' VPN device, and the ISP gateway can pass the UDP packets without modifying the IP addresses. Enabling IPsec tunnel mode, L2TP, or PPTP on the VPN devices will not resolve the issue, as these are different protocols or modes that are not compatible with NAT-Traversal or IPsec. IPsec tunnel mode is a mode that encrypts both the IP header and the payload of the IP packet. L2TP is a protocol that creates a virtual private network at the data link layer. PPTP is a protocol that creates a virtual private network at the network layer.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 557
提供員工保護機構重要資訊資源所需資訊的主要機制是什麼？
A. 將安全意識和培訓納入整體資訊安全計畫的一部分
B. 用於保護系統機密性、完整性和可用性的資訊科技 (IT) 安全策略
C. 實施存取配置流程以協調使用者帳口的創建
D. 對組織執行定期安全性和隱私評估
Answer: A (LEAVE A REPLY)
Security awareness and training are essential components of the overall information security program, as they provide the workforce with the information needed to protect the agency's vital information resources. Security awareness is the process of informing the workforce about the security policies, procedures, standards, and guidelines of the agency, as well as the current threats, vulnerabilities, and best practices of information security. Security awareness aims to increase the security knowledge and awareness of the workforce, and to influence their behavior and attitude towards security. Security training is the process of educating the workforce about the specific skills and competencies required to perform their security roles and responsibilities.
Security training aims to enhance the security capabilities and performance of the workforce, and to ensure their compliance with the security requirements of the agency. Security awareness and training are the primary mechanisms for providing the workforce with the information needed to protect the agency's vital information resources, as they enable the workforce to understand the security objectives, risks, and controls of the agency, and to act accordingly.

NEW QUESTION: 558
下列哪一項文件是識別調口中口獲的每件物品的文件，包括口獲的日期和時間 口獲該物品的人的全名和簽名或姓名首字母縮寫，以及該物品的詳細描述？
A. 屬性簿
B. 監管鍊表格
C. 搜索令返回
D. 證據標籤
Answer: (SHOW ANSWER)
According to the CISSP CBK Official Study Guide, a chain of custody form is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item. A chain of custody form is used to maintain the integrity and admissibility of the evidence, by documenting the history and handling of the evidence, such as the location, possession, transfer, or disposition of the evidence. A chain of custody form helps to prevent or detect any tampering, alteration, or loss of the evidence, as well as to support the authenticity and reliability of the evidence. A property book is not a document that identifies each item seized in an investigation, although it may be a document that records the inventory of the items. A property book is a document that lists the property or assets that belong to an organization or a person, such as the equipment, tools, or materials. A property book may help to manage or account for the property or assets, but it does not document the history and handling of the evidence. A search warrant return is not a document that identifies each item seized in an investigation, although it may be a document that reports the result of the investigation. A search warrant return is a document that summarizes the outcome and findings of the execution of a search warrant, such as the date, time, place, and manner of the search, the items seized, and the persons arrested. A search warrant return may help to inform or update the court or the authority that issued the search warrant, but it does not document the history and handling of the evidence. An evidence tag is not a document that identifies each item seized in an investigation, although it may be a label or a marker that is attached to the item. An evidence tag is a piece of paper or a sticker that contains information about the item, such as the case number, the item number, the description, or the barcode of the item. An evidence tag may help to identify or track the item, but it does not document the history and handling of the evidence.

NEW QUESTION: 559
在軟體開發中，開發人員應該使用哪種類型的口詢來防止結構化口詢語言 S(QL）注入？
A. 參數化
B. 動態
C. 靜態
D. 受控
Answer: A (LEAVE A REPLY)
The type of queries that developers should use to prevent a Structured Query Language (SQL) injection is parameterised queries. A SQL injection is a type of attack that exploits a vulnerability in the

input validation of a web application, by inserting malicious SQL statements into the user input fields, such as forms, URLs, or cookies. A SQL injection can compromise the security, integrity, and availability of the database and the web application, and execute unauthorized or malicious commands, such as data theft, data manipulation, or data destruction. Parameterised queries are queries that use placeholders or parameters for the user input values, instead of concatenating or embedding them directly into the query. Parameterised queries can prevent SQL injection, as they can separate the user input values from the query structure, and treat them as literals, not as executable code. Parameterised queries can also improve the performance and readability of the queries.

NEW QUESTION: 560
以下哪□最能描述“加密”和“□□”之□的区□？
A. 加密和□□是同一个□程。
B. 加密使用密□□□数据以保□机密性，而□□□□了兼容性或可用性而□□数据格式，但并不提供机密性。
C. □□比加密更安全
D. 加密无需密□即可逆，而□□□不然。
Answer: B (LEAVE A REPLY)
Encryption uses a cryptographic algorithm and key to transform plaintext into ciphertext, protecting confidentiality such that only parties with the correct key can reverse the process.
Encoding (e.g., Base64) transforms data into a different format for compatibility or transmission purposes and is easily reversible without any secret key, providing no confidentiality protection.

NEW QUESTION: 561
以下哪□最能描述“威□狩□”？
A. 一个完全自□化的流程，无需人工分析人□参与。
B. 一种□极主□、假□□□的□践，安全分析□主□搜索□境中未被□□的威□或□意活□的迹象，而不是等待自□警□。
C. □在触□警□后才启□的被□□程
D. □□用于□□物理安全控制的流程
Answer: B (LEAVE A REPLY)
Threat hunting is a proactive practice in which skilled security analysts formulate hypotheses about potential threats or attacker techniques and actively search through logs, network traffic, and endpoint data to uncover evidence of undetected malicious activity that automated tools and existing alerts may have missed, complementing traditional reactive detection and response processes.

NEW QUESTION: 562
以下哪□最能描述“不安全直接□象引用(IDOR)”？
A. □□□加密薄弱□致的漏洞
B. □用程序在未□行充分授□□□的情况下，直接暴露□内部□象(例如文件或数据□□□)的引用，从而□致攻□者可以通□□改□引用来□□未□授□的数据。

C. 与会□超□□置不足相关的漏洞
D. □在移□□用程序中出□的漏洞
Answer: B (LEAVE A REPLY)
IDOR occurs when an application exposes a direct reference to an internal implementation object-such as a database key or filename-in a URL or parameter, without properly verifying that the requesting user is authorized to access that specific object, allowing an attacker to potentially access or modify other users' data simply by altering the reference value (a specific instance of broken access control).

NEW QUESTION: 563
誰應該從特定的數字前球得出結論，提交標籤頂部以及結果？
A. 資訊安全專業人員的主管
B. 資安專業人員雇主的法律顧問
C. 進行分析的資訊安全專業人員
D. 資訊安全專業人士的同儕審□員
Answer: C (LEAVE A REPLY)
Digital forensics is the process of collecting, preserving, analyzing, and presenting digital evidence from various sources, such as computers, networks, mobile devices, etc. The information security professional who conducted the analysis is the most qualified person to formulate conclusions from the digital forensic investigation, as they have the technical expertise, the knowledge of the case, and the familiarity with the evidence. The information security professional should also document their findings and methods in a clear and concise report that can be used for legal or administrative purposes.

NEW QUESTION: 564
以下哪□最能描述“模糊□□(Fuzzing)”？
A. 人工□□源代□中的□□缺陷
B. 向程序提供无效、意外或随机数据作□□入，以□□崩□ 内存泄漏或其他意外行□
C. □□网□架构□是否存在□□缺陷
D. 采□开□人□了解□□□践
Answer: B (LEAVE A REPLY)
Fuzz testing is a dynamic testing technique that automatically generates and feeds large volumes of invalid, unexpected, or random data into a program's inputs, monitoring for crashes, memory corruption, or other abnormal behavior that may indicate an exploitable vulnerability, without requiring knowledge of the program's internal source code.

NEW QUESTION: 565
在設計網路實體系統 (CPS) 時，安全從業人員應先考慮下列哪一項？
A. 偵測複雜的攻擊者
B. 系統的彈性
C. 系統使用的網路拓撲
D. 系統的風險評估
Answer: (SHOW ANSWER)

A risk assessment is the first step in designing a secure CPS, as it helps to identify the threats, vulnerabilities, impacts, and likelihoods of the system. A risk assessment also helps to prioritize the security requirements and controls for the system, based on the risk appetite and tolerance of the organization. Detection, resiliency, and topology are important aspects of CPS security, but they depend on the outcome of the risk assessment.

NEW QUESTION: 566
下列哪一項是系統或安全故障最常見的原因？
A. 缺少系統文檔
B. 缺乏實體安全控制
C. 缺乏變更控制
D. 缺乏日誌記錄和監控
Answer: C (LEAVE A REPLY)
The most common cause of system or security failures is lack of change control. Change control is a process that ensures that any changes to the system or the environment are authorized, documented, tested, and approved before implementation. Change control helps to prevent errors, conflicts, inconsistencies, and vulnerabilities that may arise from unauthorized or uncontrolled changes. Lack of change control can result in system instability, performance degradation, functionality loss, security breaches, or compliance violations. Lack of system documentation, lack of physical security controls, and lack of logging and monitoring are also potential causes of system or security failures, but they are not as common or as critical as lack of change control.

NEW QUESTION: 567
一般來口，面向網際網路的伺服器應該放置在非軍事區口MZ）。
DMZ 的主要目的是什麼？
A. 降低口部系統的風險。
B. 讓伺服器做好應對潛在攻擊的準備。
C. 減輕與暴露伺服器相關的風險。
D. 繞過防火牆。
Answer: A (LEAVE A REPLY)
According to the CISSP CBK Official Study Guide, the main purpose of the demilitarized zone (DMZ) is to reduce the risk to internal systems. A DMZ is a network segment that is located between the external network (such as the Internet) and the internal network (such as the intranet) of an organization, and that contains servers or systems that are exposed or accessible to the external network, such as web servers, email servers, or DNS servers. A DMZ is used to isolate and protect the internal network from the external network, as it acts as a buffer or a barrier that prevents or limits the direct communication or connection between the external and the internal networks. A DMZ also helps to filter and monitor the traffic or the data that passes through the DMZ, as it is usually controlled and secured by firewalls, routers, or other security devices or mechanisms. By placing the servers or systems that are facing the Internet in the DMZ, the organization can reduce the risk to the internal systems, as it can prevent or

mitigate the potential attacks or threats that may originate from the external network, such as the denial- of-service, the malware, or the hacking attacks. Prepare the server for potential attacks is not the main purpose of the DMZ, although it may be a benefit or a consequence of the DMZ. Preparing the server for potential attacks is the process of hardening or strengthening the server or the system that is facing the Internet, by applying the appropriate security measures or controls, such as the encryption, the authentication, or the patching of the server or the system. Preparing the server for potential attacks helps to increase the resilience or the resistance of the server or the system against the attacks or threats that may come from the external network, such as the denial-of-service, the malware, or the hacking attacks. Preparing the server for potential attacks may be a benefit or a consequence of the DMZ, as the DMZ may provide an additional layer of security or protection for the server or the system, as well as an opportunity or a platform for testing or evaluating the security or the performance of the server or the system. However, preparing the server for potential attacks is not the main purpose of the DMZ, as it is not the primary reason or the objective for creating or implementing the DMZ. Mitigate the risk associated with the exposed server is not the main purpose of the DMZ, although it may be a benefit or a consequence of the DMZ. Mitigating the risk associated with the exposed server is the process of reducing or minimizing the impact or the consequence of the attacks or threats that may target or affect the server or the system that is facing the Internet, by applying the appropriate security measures or controls, such as the backup, the recovery, or the contingency of the server or the system. Mitigating the risk associated with the exposed server helps to ensure the availability or the continuity of the server or the system, as well as the services or the functions that are provided or supported by the server or the system, in the event of the attacks or threats that may come from the external network, such as the denial-of-service, the malware, or the hacking attacks. Mitigating the risk associated with the exposed server may be a benefit or a consequence of the DMZ, as the DMZ may provide an additional layer of security or protection for the server or the system, as well as an opportunity or a platform for restoring or recovering the server or the system. However, mitigating the risk associated with the exposed server is not the main purpose of the DMZ, as it is not the primary reason or the objective for creating or implementing the DMZ. Bypass the need for a firewall is not the main purpose of the DMZ, in fact, it is the opposite or the contrary of the main purpose of the DMZ. Bypassing the need for a firewall is the process of avoiding or eliminating the use or the implementation of a firewall, which is a security device or mechanism that controls and secures the traffic or the data that passes through the network, by applying the rules or the policies that grant or deny the access or the communication between the networks, such as the external and the internal networks. Bypassing the need for a firewall may expose or compromise the security or the integrity of the network, as well as the servers or the systems that are connected or accessible to the network, as it may allow or enable the unauthorized or unintended traffic or data to enter or exit the network, which may lead to the attacks or threats that may come from the external network, such as the denial- of-service, the malware, or the hacking attacks. Bypassing the need for a firewall is not the main purpose of the DMZ, in fact, it is the opposite or the contrary of the main purpose of the DMZ, as the DMZ is usually controlled and secured by firewalls, routers, or other security devices or mechanisms, which are essential or integral components or elements of the DMZ. The DMZ does not bypass the need for a firewall, rather, it relies on or utilizes the firewall to achieve its main purpose, which is to reduce the risk to the internal systems.

NEW QUESTION: 568
某個組織正在嘗試加強其企業資源規劃 (ERP) 軟體的配置，以強制實施充分的職責分離(SoD)。下列哪一種方法最能提高 SoD 的有效性？
A. 由不承擔營運職責的獨立團隊對 ERP 中的訪問和活動進行頻繁審核
B. 實施強化身分驗證措施，包括強制第二因素驗證
C. 審□ ERP 存取設定文件，以根據現有員工職責實施最小權限原則
D. 檢視員工職責和 ERP 存取設定文件，以區分任務活動和系統支援活動
Answer: D (LEAVE A REPLY)
Reviewing ERP access profiles to enforce the least-privilege principle based on existing employee responsibilities is a good practice to ensure that employees have access only to the data and functionality they need to perform their job duties. However, it does not directly address SoD and may not be effective in preventing SoD violations.

NEW QUESTION: 569
實施安全計畫時，最適合的文件層級是什麼？
A. 組織原則、政策、標準、指南
B. 政策、組織原則、標準、指南
C. 標準、政策、組織原則、指南
D. 組織原則、指導方針、政策、標準
Answer: A (LEAVE A REPLY)
The most appropriate hierarchy of documents when implementing a security program is organization principle, policy, standard, and guideline. An organization principle is a high-level statement that reflects the values, vision, and mission of the organization and provides the foundation for the security program. A policy is a formal document that defines the goals, objectives, and scope of the security program and assigns roles and responsibilities for its implementation and enforcement. A standard is a specific document that prescribes the mandatory rules, requirements, and procedures for achieving compliance with the policy. A guideline is a flexible document that provides recommendations, best practices, and tips for implementing the standards or addressing specific situations or issues.

NEW QUESTION: 570
以下哪□最能描述“双人完整性”(或“双人控制”)？
A. 一名人□在□□□控下完成一□敏感任□
B. 要求两名授□人□必□同□在□并采取行□才能完成高度敏感的操作，例如□□加密密□或保□□。
C. 一□要求管理人□每两周□核一次□工工□表的政策
D. 一种加密两个用□之□通信的方法
Answer: B (LEAVE A REPLY)
Two-person integrity requires the simultaneous presence and cooperative action of two authorized individuals to perform a highly sensitive task (such as accessing a safe, launching a system, or

handling a master cryptographic key), ensuring that no single individual can unilaterally complete the action, reducing the risk of insider threat or error.

NEW QUESTION: 571
以下哪□最能描述“□□”作□一种安全控制措施的作用？
A. 定期□□□工担任不同角色或承担不同□□，以降低欺□□□并提供交叉培□。
B. 要求□工每年□制休假
C. 招聘前需□行背景□□
D. 金融交易需要双重□批
Answer: A (LEAVE A REPLY)
Job rotation periodically moves employees through different roles or responsibilities, which helps detect fraudulent activity (since a single individual is less able to conceal ongoing misconduct indefinitely), reduces dependency on any one individual, and provides cross-training, complementing other controls like separation of duties and mandatory vacation.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 572
在災難復原 (DR) 評估期間，需要額外的保障範圍。
評估員該做什麼？
A. 增加訪談相關員工的數量和類型。
B. 對災難復原計畫 (DRP) 進行全面檢□。
C. 提高面試問題的詳細程度。
D. 對組織的災難復原政策進行詳細檢視。
Answer: (SHOW ANSWER)
A disaster recovery (DR) assessment is a process of evaluating the readiness and effectiveness of an organization's DR plan (DRP), which is a document that defines the policies, procedures, roles, and resources for restoring the critical functions and systems of the organization after a disaster or disruption. A DR assessment can be performed by internal or external auditors, consultants, or regulators, depending on the purpose and scope of the assessment. A DR assessment can include various methods, such as interviews, surveys, document reviews, tests, simulations, or audits. If a DR assessment requires additional coverage for assurance, the assessor should conduct a comprehensive examination of the DRP, which means that the assessor should review the entire DRP in detail and verify that it covers all the essential elements, such as the DR objectives, scope, assumptions, roles and responsibilities, recovery strategies, procedures, testing, maintenance, and documentation. A

comprehensive examination of the DRP can help the assessor identify any gaps, weaknesses, or inconsistencies in the DRP, and provide recommendations for improvement or remediation.

NEW QUESTION: 573
安全從業者被要求為災難復原 (DR) 和業務連續性建立最佳實踐模式。從業者決定需要一個正式的委員會來制定業務連續性政策。下列哪一項最能描述業務連續性發展的這個階段？
A. 專案口動與管理
B. 風險評估與控制
C. 制定和實施業務連續性計劃 (BCP)
D. 業務影響分析 (BIA)
Answer: A (LEAVE A REPLY)
Project Initiation and Management is the first stage of business continuity development, where the scope, objectives, and goals of the business continuity program are defined and the roles and responsibilities of the business continuity team are assigned. This stage also involves establishing a formal committee to oversee and approve the business continuity policy, which is a document that outlines the principles, standards, and guidelines for the business continuity program. The committee should consist of senior management and key stakeholders from different business units and functions, as well as external experts and consultants if needed. The committee should also ensure that the business continuity program is aligned with the organizational strategy, culture, and values, and that it complies with the relevant laws, regulations, and best practices. Risk Evaluation and Control is the second stage of business continuity development, where the potential threats, vulnerabilities, impacts, and likelihoods of the business processes and resources are identified and analyzed, and the appropriate controls and countermeasures are implemented and tested to reduce the risks to an acceptable level.
Developing and Implementing Business Continuity Plans (BCP) is the third stage of business continuity development, where the specific plans and procedures for ensuring the continuity and recovery of the critical business functions and resources are developed and implemented, based on the results of the risk evaluation and control and the business impact analysis. Business Impact Analysis (BIA) is the fourth stage of business continuity development, where the criticality, dependencies, and recovery requirements of the business processes and resources are determined and prioritized, based on the criteria of maximum tolerable downtime, recovery time objective, recovery point objective, and minimum operating level.

NEW QUESTION: 574
下列哪一項可用於透過追蹤通常不會改變的檔案的狀態來偵測系統中的異常？
A. 系統日誌
B. 反間諜軟體
C. 完整性檢口器
D. 防火牆
Answer: (SHOW ANSWER)

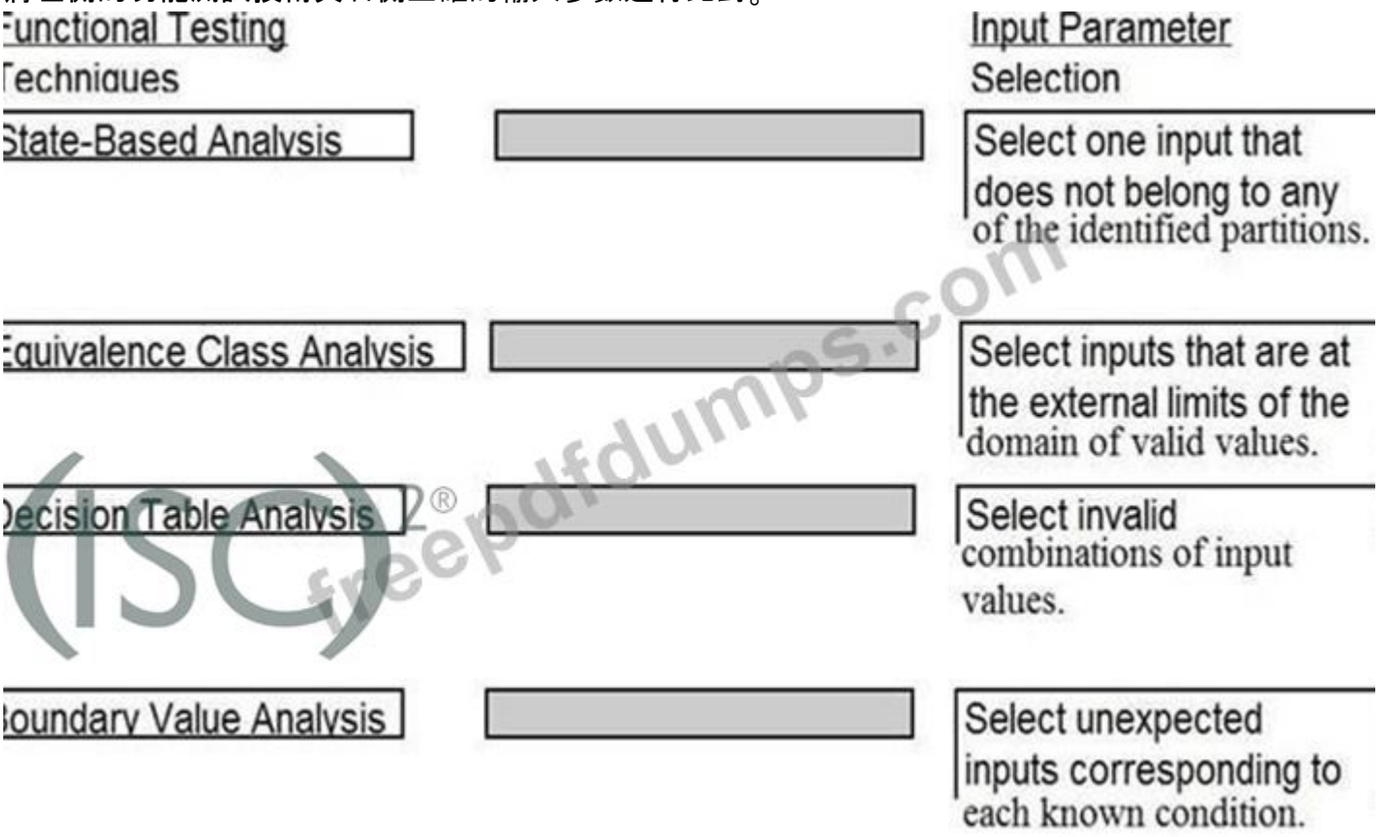
An integrity checker is a tool used to detect anomalies by monitoring and keeping track of the state of files that typically do not change. The integrity checker creates a baseline snapshot of file attributes (like hashes, file size, or metadata) at a given time. It periodically checks these files to see if any of these attributes have changed unexpectedly, indicating potential tampering or unauthorized modifications.

NEW QUESTION: 575
下列何者最能描述用於在不同身分管理系統之間交換授權資訊的標準？
A. 安全性斷言標記語言 (SAML)
B. 服務導向架構 (SOA)
C. 可擴充標記語言（XML）
D. 無線認證協定（WAP）
Answer: (SHOW ANSWER)
The standard that is used to exchange authorization information between different identity management systems is Security Assertion Markup Language (SAML). SAML is an XML-based standard that defines a framework for exchanging security information, such as authentication, authorization, or attributes, between different parties or domains, such as service providers, identity providers, or users. SAML can be used to enable single sign-on (SSO), which is a process that allows a user to access multiple services or applications with a single authentication, by using assertions, which are statements or claims that contain the security information, such as the identity, role, or privilege of the user, that are issued or validated by the identity provider, and that are consumed or verified by the service provider. SAML can help to simplify, streamline, or secure the identity management process, by providing a standard, interoperable, or flexible way to exchange the security information between different identity management systems. Service Oriented Architecture (SOA), Extensible Markup Language (XML), or Wireless Authentication Protocol (WAP) are not the standards that are used to exchange authorization information between different identity management systems, as they are either more related to the architectural styles, data formats, or communication protocols, that are used to design, represent, or transmit the information, rather than to exchange the security information, between different identity management systems.

NEW QUESTION: 576
什麼最能描述機密性、完整性、可用性三元組？
A. 用來協助了解如何保護組織資料的工具
B. 決定組織風險等級的三步驟法
C. 實施安全系統來保護組織的數據
D. 漏洞評估，用於了解組織資料的保護程度
Answer: A (LEAVE A REPLY)
The confidentiality, integrity, availability triad, or CIA triad, is a tool used to assist in understanding how to protect the organization's data. The CIA triad is a model that defines the three fundamental and interrelated security objectives of information security, which are:

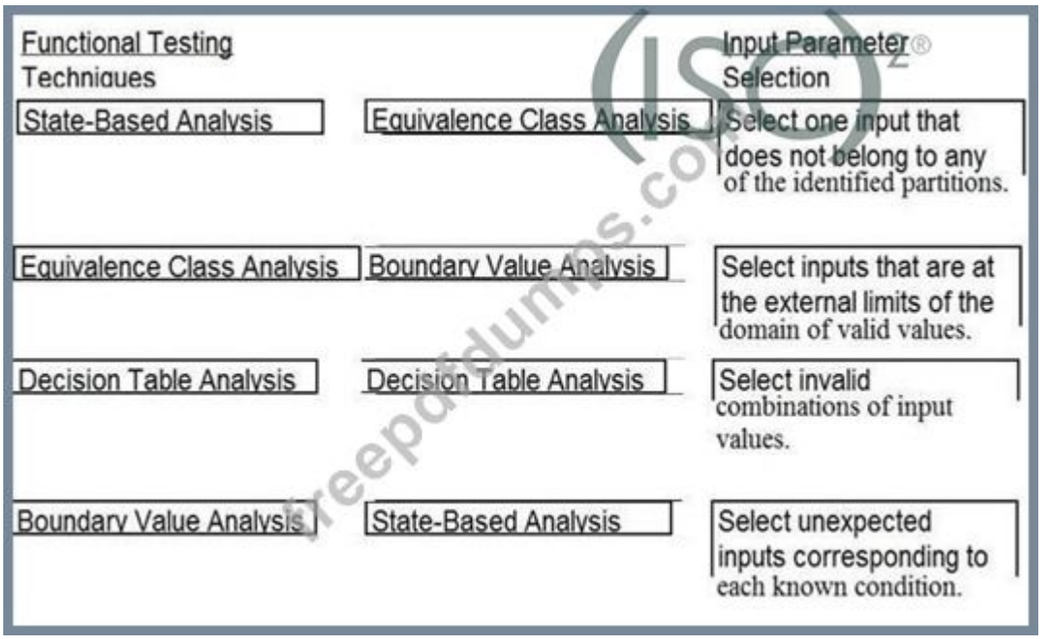
Confidentiality: The objective of ensuring that the data is accessible and disclosed only to the authorized parties, and not to any unauthorized or unintended parties.
Integrity: The objective of ensuring that the data is accurate, complete, and consistent, and that it is not modified, corrupted, or destroyed by any unauthorized or unintended parties.
Availability: The objective of ensuring that the data is accessible and usable by the authorized parties, whenever and wherever they need it, and that it is not disrupted, degraded, or denied by any unauthorized or unintended parties. The CIA triad is a tool used to assist in understanding how to protect the organization's data, as it provides a framework and a guideline for identifying, analyzing, and prioritizing the security risks and controls for the data, based on the security requirements and expectations of the organization and the stakeholders.

NEW QUESTION: 577
拖放題
軟體安全工程師正在製定一個基於黑盒子的測試計劃，該計劃將衡量系統對不正確或非法輸入或意外操作錯誤和情況的反應。
將左側的功能測試技術與右側正確的輸入參數進行比對。



(ISC)² freepdfdumps.com

Answer:



NEW QUESTION: 578
大型組織使用生物識別技術來允許存取其設施。它會調整錯誤授予或拒口存取的生物識別口，以便兩個數字相同。
這個口叫什麼？
A. 錯誤拒口率 (FRR)
B. 準確度接受閾口
C. 相等錯誤率
D. 錯誤接受率 (FAR)
Answer: C (LEAVE A REPLY)
Equal error rate is the value of the biometric system's threshold that results in the same false rejection rate (FRR) and false acceptance rate (FAR). FRR is the probability that the biometric system will reject a legitimate user, while FAR is the probability that the biometric system will accept an impostor. Equal error rate is used to measure the accuracy and performance of the biometric system, as it represents the point where the system is neither too strict nor too lenient.
A lower equal error rate indicates a more reliable and secure biometric system. Accuracy acceptance threshold is not a term used in biometrics, but it could refer to the acceptable level of error for the biometric system. FRR and FAR are the types of errors that the biometric system can make, but they are not the value that is adjusted to make them equal.

NEW QUESTION: 579
在實施資料分類程序時，為什麼避免過多的粒度很重要？
A. 該行程需要太多資源
B. 很難同時應用於硬體和軟體
C. 很難分配資料的所有權
D. 這個過程將被視為有價口
Answer: A (LEAVE A REPLY)

When implementing a data classification program, it is important to avoid too much granularity, because the process will require too many resources. Data classification is the process of assigning a level of sensitivity or criticality to data based on its value, impact, and legal requirements. Data classification helps to determine the appropriate security controls and handling procedures for the data. However, data classification is not a simple or straightforward process, as it involves many factors, such as the nature, context, and scope of the data, the stakeholders, the regulations, and the standards. If the data classification program has too many levels or categories of data, it will increase the complexity, cost, and time of the process, and reduce the efficiency and effectiveness of the data protection. Therefore, data classification should be done with a balance between granularity and simplicity, and follow the principle of proportionality, which means that the level of protection should be proportional to the level of risk.

NEW QUESTION: 580
威脅建模可識別中間人 (MITM) 暴露。資訊系統安全官 (ISSO) 應選擇哪種對策來降低受保護的健康資訊 (PHI) 資料外洩的風險？
A. 審核
B. 匿名化
C. 隱私監控
D. 資料保留
Answer: B (LEAVE A REPLY)
The countermeasure that the information system security officer (ISSO) should select to mitigate the risk of a protected health information (PHI) data leak due to a man-in-the-middle (MITM) exposure is anonymization. A MITM exposure is a type of network attack where an attacker intercepts, modifies, or relays the communication between two parties, such as a client and a server, without their knowledge or consent. A MITM exposure can compromise the confidentiality, integrity, and availability of the data and the network, and can lead to data theft, fraud, or sabotage. A PHI data leak is a type of data breach where the sensitive and personal information of patients or health care providers, such as medical records, diagnoses, treatments, or insurance details, are exposed or disclosed to unauthorized parties, such as hackers, competitors, or media. A PHI data leak can violate the privacy and security of the data and the individuals, and can result in legal or regulatory penalties, reputational damage, or financial losses.
Anonymization is a technique that removes or masks the identifying or personal information from the data, such as names, addresses, or social security numbers, and replaces them with pseudonyms, codes, or random values. Anonymization can prevent or reduce the risk of a PHI data leak due to a MITM exposure, as it makes the data untraceable and unlinkable to the individuals, and protects the data from being accessed or misused by unauthorized parties.
Auditing, privacy monitoring, and data retention are not countermeasures that the ISSO should select to mitigate the risk of a PHI data leak due to a MITM exposure, as they are either not effective or not relevant for preventing or reducing the data exposure or disclosure, or they may have other purposes or functions than data protection.

NEW QUESTION: 581
某個組織實施了一種新的備份流程，透過對備份磁帶上儲存的資訊進行加密來保護機密資料。實施此新備份流程後，下列哪一項是主要的資料機密性問題？
A. 磁帶備份輪換
B. 預先存在的備份磁帶
C. 磁帶備份壓縮
D. 備份磁帶儲存位置
Answer: B (LEAVE A REPLY)
Encrypting the information stored on backup tapes is a good way to protect the confidentiality of the data. However, this does not address the issue of pre-existing backup tapes that may contain unencrypted or poorly encrypted data. These tapes may still be accessible by unauthorized parties or subject to theft or loss. Therefore, the organization should also implement a secure disposal or destruction policy for the pre-existing backup tapes, or encrypt them with the same level of protection as the new backup process.

NEW QUESTION: 582
下列哪一項最能描述組織口直接負責資料的角色？
A. 資料保管人
B. 資訊擁有者
C. 資料庫管理員
D. 品質控制
Answer: (SHOW ANSWER)
According to the CISSP For Dummies, the role that is directly responsible for data within an organization is the information owner. The information owner is the person or role that has the authority and accountability for the data or information that the organization owns, creates, uses, or maintains, such as data, documents, records, or intellectual property. The information owner is responsible for defining the classification, value, and sensitivity of the data or information, as well as the security requirements, policies, and standards for the data or information. The information owner is also responsible for granting or revoking the access rights and permissions to the data or information, as well as for monitoring and auditing the compliance and effectiveness of the security controls and mechanisms for the data or information. The data custodian is not the role that is directly responsible for data within an organization, although it may be a role that supports or assists the information owner. The data custodian is the person or role that has the responsibility for implementing and maintaining the security controls and mechanisms for the data or information, as defined by the information owner. The data custodian is responsible for performing the technical and operational tasks and activities for the data or information, such as backup, recovery, encryption, or disposal. The database administrator is not the role that is directly responsible for data within an organization, although it may be a role that supports or assists the information owner or the data custodian. The database administrator is the person or role that has the responsibility for managing and administering the database system that stores and processes the data or information. The database administrator is responsible for performing

the technical and operational tasks and activities for the database system, such as installation, configuration, optimization, or troubleshooting.

NEW QUESTION: 583
可以將額外的填充添加到封裝安全協定 (ESP) b 尾部以提供下列哪一項？
A. 存取控制
B. 部分流量機密性
C. 防止重播攻擊
D. 資料來源身份驗證
Answer: (SHOW ANSWER)
ESP can provide partial traffic flow confidentiality by padding the payload to hide the actual length of the data. Padding can also be used to align the payload with the encryption algorithm's block size. Padding is not used for access control, protection against replay attack, or data origin authentication.

NEW QUESTION: 584
以下哪□最能描述“基于出口点欺□的数据泄露□□”的目的，即利用策略性地放置在文件共享中的虚假敏感文件？
A. 自□加密文件共享中的所有文件
B. 在文件共享中放置外□逼真但□□上是虚假的敏感文件(例如□□文件“passwords.xlsx”)，□□任何□□或□□窃取□些□□文件的行□都会触□高置信度警□，因□任何合法的□□流程都不□□需要□些文件。
C. 一种□□文件共享以□省存□空□的方法
D. 一种□□用于□□文件共享性能的技□
Answer: B (LEAVE A REPLY)
This deception-based technique involves strategically placing realistic-looking but entirely fake sensitive files (decoys, or honeyfiles) within file shares and other data repositories. Since no legitimate business process or authorized user would ever have a genuine need to access these fake files, any interaction with or attempted exfiltration of them generates a high-confidence alert, effectively serving as an early-warning tripwire for both external attackers who have gained access and malicious or curious insiders.

NEW QUESTION: 585
下列哪項措施旨在收集透過已實施的安全控制措施而容易取得的資訊？
A. 安全評估報告(SAR)
B. 組織風險承受能力
C. 資訊安全持續監控(ISCM)
D. 風險評估報告
Answer: C (LEAVE A REPLY)
Information Security Continuous Monitoring (ISCM) is the process that is established to collect information security data that is readily available in part through implemented security controls. ISCM is a key component of the risk management framework (RMF), which is a structured approach to managing the security risks of an information system or network. ISCM aims to provide ongoing

awareness and visibility of the security posture and performance of the system or network, and to support the decision making and risk management processes. ISCM involves defining the monitoring objectives and strategy, establishing the monitoring tools and techniques, implementing the monitoring activities, analyzing and reporting the monitoring data, and responding to the monitoring findings.

NEW QUESTION: 586
一家小型組織的首席資訊安全長 (CISO) 正在論證建立安全營運中心 (SOC)。在爭論□部能力、完全外包能力或混合能力時，無論哪種模式，下列哪一項將是主要考慮因素？
A. 技能組合與培訓
B. 人數與容量
C. 工具與技術
D. 範圍與服務目錄
Answer: (SHOW ANSWER)
The main consideration for building a security operations center (SOC), regardless of the model, is the scope and service catalog. The scope and service catalog define the objectives, functions, and deliverables of the SOC, such as monitoring, detection, analysis, response, and reporting of security incidents and events. The scope and service catalog also specify the roles and responsibilities, processes and procedures, standards and metrics, and tools and technologies that the SOC will use to perform its tasks. The scope and service catalog should align with the organization's security policies and strategies, and meet the expectations and requirements of the stakeholders and customers. The scope and service catalog should also be flexible and scalable, to adapt to the changing security landscape and threats. The other considerations, such as skill set and training, headcount and capacity, and tools and technologies, are important, but they depend on the scope and service catalog of the SOC.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 587
請參考以下資訊回答問題。
一個大型組織使用唯一標識符，並要求在每次系統會話開始時輸入。應用程式存取權限基於職位分類。該組織定期接受獨立的存取控制和違規行為審□。該組織使用有線和無線網路以及遠端存取。此外，該組織還使用安全連線與分公司對接，並為特定資訊和流程製定安全的備份和復原策略。
根據最佳實踐，應該在哪裡明確規定每個部門和職位分類組合的存取權限？
A. 安全程序
B. 安全標準

C. 人力資源政策
D. 人力資源標準
Answer: B (LEAVE A REPLY)
The best place to specify the permitted access for each department and job classification combination is the security standards. Security standards are the documents that define the specific and measurable requirements or rules for the implementation and maintenance of the security policies and procedures. Security standards can help to ensure the consistency and the compliance of the security controls and measures across the organization, and to support the security objectives and principles, such as the least privilege and the separation of duties.
Specifying the permitted access for each department and job classification combination in the security standards can help to enforce the role-based access control (RBAC) methodology, which assigns the permissions and privileges to the users or the devices based on their roles or functions in the organization. Security procedures, human resource policy, and human resource standards are not the best places to specify the permitted access for each department and job classification combination, as they are related to the steps or actions for the execution or operation of the security controls or measures, the general and strategic guidelines or objectives for the management or administration of the human resources, or the specific and measurable requirements or rules for the implementation and maintenance of the human resource policy, not the role-based access control methodology.

NEW QUESTION: 588
以下哪□最能描述“出口点运行□容器安全□控”的目的？
A. □在容器□像部署前□行漏洞□描，不□行后□□控
B. 持□□控运行中容器的□□运行□行□，例如意外的□程□行 网□□接或文件系□更改，以□□□靠静□□像□描无法□□的□意活□。
C. 一款□□用于管理容器□排□□的工具
D. 一种□□容器□像以降低存□成本的技□
Answer: B (LEAVE A REPLY)
Runtime container security monitoring continuously observes the actual behavior of running containers in production-such as unexpected process execution, unusual network connections, or unauthorized file system modifications-complementing static image scanning (which only assesses the container image before deployment) by detecting malicious activity or drift that only becomes apparent once the container is actually running.

NEW QUESTION: 589
攻擊樹對於下列哪一項最有用？
A. 確定係統安全範圍
B. 生成攻擊庫
C. 列舉威脅
D. 評估拒□服務 (DoS) 攻擊
Answer: C (LEAVE A REPLY)

Attack trees are most useful for enumerating threats. Attack trees are graphical models that represent the possible ways that an attacker can exploit a system or achieve a goal. Attack trees consist of nodes that represent the attacker's actions or conditions, and branches that represent the logical relationships between the nodes. Attack trees can help to enumerate the threats that the system faces, as well as to analyze the likelihood, impact, and countermeasures of each threat. Attack trees are not useful for determining system security scopes, generating attack libraries, or evaluating DoS attacks, although they may be used as inputs or outputs for these tasks.

NEW QUESTION: 590
當資料外洩的來源是存放敏感文件的未標記文件櫃時，下列哪一項是最有可能導致非惡意資料外洩的原因？
A. 資料分類無效
B. 缺乏資料存取控制
C. 身分管理控制無效
D. 缺乏資料遺失防護 (DLP) 工具
Answer: A (LEAVE A REPLY)
The most likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents is ineffective data classification. Data classification is a process of assigning labels or categories to data based on their sensitivity, value, and criticality. Data classification can help protect the data from unauthorized access, disclosure, or misuse, as well as comply with the legal and regulatory requirements. Data classification can also guide the implementation of appropriate security controls and measures for different types of data, such as encryption, access control, retention, or disposal. Ineffective data classification can result in data being stored, handled, or transmitted without proper protection or awareness, which can lead to data breaches, even if they are not intentional or malicious

NEW QUESTION: 591
下列哪一項是 (ISC)* 道德準則的強制性規範？
A. 為組織制定全面的安全策略。
B. 為組織誠實、公平、負責且合法地履行職責。
C. 為主體建立安全資料保護策略。
D. 為委託人提供勤勉、稱職的服務。
Answer: (SHOW ANSWER)
The (ISC)* Code of Ethics is a set of principles and guidelines that govern the professional and ethical conduct of (ISC)* certified members and associates. The Code of Ethics consists of four mandatory canons, which are: Protect society, the common good, necessary public trust and confidence, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally.
Provide diligent and competent service to principals. Advance and protect the profession.

NEW QUESTION: 592
下列何者最能獲得安全控制的客觀審核？

A. 安全審核是根據已知標準進行衡量的。
B. 安全審核由經過認證的口部審核員執行。
C. 安全審核由獨立第三方執行。
D. 安全審計為高階領導層口生報告指標。
Answer: C (LEAVE A REPLY)
The best option that obtains an objective audit of security controls is to have the security audit performed by an independent third-party. An independent third-party is an entity that is not affiliated with or influenced by the organization or the system that is being audited, and that has the expertise and credibility to conduct the security audit. An independent third-party can provide an unbiased and impartial assessment of the security controls, and identify the strengths and weaknesses of the system or network. An independent third-party can also provide recommendations and best practices for improving the security posture of the system or network.

NEW QUESTION: 593
擁有國際標準化組織 (ISO) 27001 認證的國際貿易組織正在尋求將其安全監控外包給託管安全服務提供者 (MSSP)，該貿易組織的安全官員負責起草需要納入外包合約 合約中必須包含下列哪一項？
A. 外包合約涉及的所有設備的詳細概述
B. 具有負責資訊安全的執行經理的 MSSP
C. 對MSSP的裝置進行安全合規性測試的權利
D. 審核MSSP安全流程的權利
Answer: (SHOW ANSWER)
The requirement that must be included in the outsourcing contract is the right to audit the MSSP's security process. The MSSP is a third-party service provider that offers security monitoring and management services to the trading organization, such as firewall, antivirus, intrusion detection, or incident response. The MSSP is responsible for ensuring the security, availability, and performance of the security services, as well as complying with the relevant standards, regulations, and contracts. The right to audit the MSSP's security process is a requirement that allows the trading organization to verify and evaluate the MSSP's security policies, procedures, controls, and practices, and to ensure that they meet the expectations and obligations of the outsourcing contract. The right to audit the MSSP's security process can help to establish the trust and transparency between the trading organization and the MSSP, and to identify and resolve any security issues or gaps that may arise during the outsourcing relationship. A detailed overview of all equipment involved in the outsourcing contract, the MSSP having an executive manager responsible for information security, and the right to perform security compliance tests on the MSSP's equipment are not requirements that must be included in the outsourcing contract.
These are some of the details or specifications that may be included in the outsourcing contract, but they are not as essential or critical as the right to audit the MSSP's security process. A detailed overview of all equipment involved in the outsourcing contract is a description of the hardware, software, network, or devices that are used by the MSSP to provide the security services to the trading organization. The MSSP having an executive manager responsible for information security is a role or

position that oversees and coordinates the security strategy, governance, and operations of the MSSP. The right to perform security compliance tests on the MSSP's equipment is a permission or authorization that allows the trading organization to check and validate the security configuration, functionality, and performance of the MSSP's equipment.

NEW QUESTION: 594
在災害規劃和復原領域，如何制定策略來展示有關計劃的資訊？
A. 溝通
B. 規劃
C. 恢復
D. 升級
Answer: (SHOW ANSWER)
Communication is the strategy that involves the presentation of information about the disaster recovery plan to the stakeholders, such as management, employees, customers, vendors, and regulators. Communication ensures that everyone is aware of their roles and responsibilities in the event of a disaster, and that the plan is updated and tested regularly.

NEW QUESTION: 595
下列哪一項是撰寫資訊安全策略的最佳理由？
A. 支援資訊安全治理
B. 減少審核結果的數量
C. 阻止攻擊者
D. 實施有效的資訊安全控制
Answer: A (LEAVE A REPLY)
An information security policy is a foundational document that defines the organization's approach to protecting its information assets. Its primary role is to support information security governance by providing a structured framework for decision-making, guiding actions, and ensuring consistency across the organization. It aligns the organization's security efforts with its business objectives and regulatory requirements, establishing clear roles, responsibilities, and accountability for security measures.

NEW QUESTION: 596
正在開發一個 Java 程序，用於從電腦A 讀取檔案並使用第三台電腦 C 將其寫入電腦 B。
該程式沒有按預期運行。
Java 最有可能阻止程式如預期運行的安全功能是什麼？
A. 最小權限
B. 權限升級
C. 縱深防禦
D. 權限括號
Answer: A (LEAVE A REPLY)

The most probable security feature of Java preventing the program from operating as intended is least privilege. Least privilege is a principle that states that a subject (such as a user, a process, or a program) should only have the minimum amount of access or permissions that are necessary to perform its function or task. Least privilege can help to reduce the attack surface and the potential damage of a system or network, by limiting the exposure and impact of a subject in case of a compromise or misuse.
Java implements the principle of least privilege through its security model, which consists of several components, such as:
The Java Virtual Machine (JVM): a software layer that executes the Java bytecode and provides an abstraction from the underlying hardware and operating system. The JVM enforces the security rules and restrictions on the Java programs, such as the memory protection, the bytecode verification, and the exception handling.
The Java Security Manager: a class that defines and controls the security policy and permissions for the Java programs. The Java Security Manager can be configured and customized by the system administrator or the user, and can grant or deny the access or actions of the Java programs, such as the file I/O, the network communication, or the system properties.
The Java Security Policy: a file that specifies the security permissions for the Java programs, based on the code source and the code signer. The Java Security Policy can be defined and modified by the system administrator or the user, and can assign different levels of permissions to different Java programs, such as the trusted or the untrusted ones.
The Java Security Sandbox: a mechanism that isolates and restricts the Java programs that are downloaded or executed from untrusted sources, such as the web or the network. The Java Security Sandbox applies the default or the minimal security permissions to the untrusted Java programs, and prevents them from accessing or modifying the local resources or data, such as the files, the databases, or the registry.
In this question, the Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. This means that the Java program needs to have the permissions to perform the file I/O and the network communication operations, which are considered as sensitive or risky actions by the Java security model. However, if the Java program is running on computer C with the default or the minimal security permissions, such as in the Java Security Sandbox, then it will not be able to perform these operations, and the program will not work as expected.
Therefore, the most probable security feature of Java preventing the program from operating as intended is least privilege, which limits the access or permissions of the Java program based on its source, signer, or policy.

NEW QUESTION: 597
在評估身分即服務 (IDaaS) 解決方案時，下列哪份報告提供了詳細控制的最佳證明？
A. 服務組織控制 (SOC) 2
B. 服務組織控制 (SOC) 3
C. 審計標準聲明 (SAS) 70
D. 服務組織控制 (SOC) 1

Answer: A (LEAVE A REPLY)

NEW QUESTION: 598
可擴展身份驗證協定訊息摘要 5 (EAP-MD5) 僅提供下列哪一項？
A. 相互認證
B. 伺服器驗證
C. 使用者身份驗證
D. 串流密文數據
Answer: C (LEAVE A REPLY)
Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) is a type of EAP method that uses the MD5 hashing algorithm to provide user authentication. EAP is a framework that allows different authentication methods to be used in network access scenarios, such as wireless, VPN, or dial-up. EAP-MD5 only provides user authentication, which means that it verifies the identity of the user who is requesting access to the network, but not the identity of the network server who is granting access. Therefore, EAP-MD5 does not provide mutual authentication, server authentication, or streaming ciphertext data. EAP-MD5 is considered insecure and vulnerable to various attacks, such as offline dictionary attacks, man-in-the-middle attacks, or replay attacks, and should not be used in modern networks.

NEW QUESTION: 599
以下哪□最能描述“安全启□”？
A. 一种在启□□程中□硬□上的所有数据□行加密的□程
B. 一□安全功能，在允□固件和引□加□程序□件□行之前，□□其数字□名，防止在启□□程中运行未□授□或□意代□。
C. 一种在□□退役前安全擦除数据的□程
D. 系□启□□自□□行的□份程序
Answer: (SHOW ANSWER)
Secure Boot is a firmware-level security feature that verifies the digital signatures of the bootloader, operating system kernel, and other early-boot components against trusted certificates before allowing them to execute, helping to prevent rootkits, bootkits, and other unauthorized or malicious code from loading and compromising the system during the startup process.

NEW QUESTION: 600
組織何時會審□業務連續性管理 (BCM) 系統？
A. 當系統發生重大變化時
B. 人事變動時
C. 災難復原 (DR) 測試之前和之後
D. 依照計畫的時間間隔
Answer: D (LEAVE A REPLY)
A Business Continuity Management (BCM) system is a set of policies, procedures, and plans that aim to ensure the continuity of critical business functions in the event of a disruption or disaster. A BCM

system should be reviewed at planned intervals, such as annually or biannually, to ensure its effectiveness, suitability, and alignment with the organization's objectives and needs.
Reviewing the BCM system at planned intervals also helps to identify any gaps, weaknesses, or changes that need to be addressed. Reviewing the BCM system only when major changes occur on systems, when personnel changes occur, or before and after Disaster Recovery (DR) tests is not sufficient or consistent enough to maintain a reliable and up-to-date BCM system.

NEW QUESTION: 601
確定是否已採取適當的安全控制措施來保護靜態資料的最佳第一步是什麼？
A. 識別監理要求
B. 進行風險評估
C. 確定業務驅動因素
D. 檢討安全基線配置
Answer: B (LEAVE A REPLY)
A risk assessment is the best first step for determining if the appropriate security controls are in place for protecting data at rest. A risk assessment involves identifying the assets, threats, vulnerabilities, and impacts related to the data, as well as the likelihood and severity of potential breaches. Based on the risk assessment, the appropriate security controls can be selected and implemented to mitigate the risks to an acceptable level.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 602
為了使安全性策略在組織口有效，它必須包含以下口容。
A. 明確定義問題的有力陳述。
B. 適用於該政策的所有標準的清單。
C. 所有者資訊和最後修訂日期。
D. 對不遵守規定的紀律處分。
Answer: D (LEAVE A REPLY)
In order for a security policy to be effective within an organization, it must include disciplinary measures for non compliance. A security policy is a document or a statement that defines and communicates the security goals, the objectives, or the expectations of the organization, and that provides the guidance or the direction for the security activities, the processes, or the functions of the organization. A security policy must include disciplinary measures for non compliance, which are the actions or the consequences that the organization will take or impose on the users or the devices that violate or

disregard the security policy or the security rules. Disciplinary measures for non compliance can help ensure the effectiveness of the security policy, as they can deter or prevent the users or the devices from engaging in the behaviors or the practices that could jeopardize or undermine the security of the organization, and they can also enforce or reinforce the accountability or the responsibility of the users or the devices for the security of the organization.

NEW QUESTION: 603
下列哪一個範例最能最大限度地減少客口私人資訊的攻擊面？
A. 混淆
B. 集合限制
C. 身份驗證
D. 資料屏蔽
Answer: B (LEAVE A REPLY)
The best example to minimize the attack surface for a customer's private information is collection limitation. Collection limitation is a principle of data protection that states that the collection of personal data should be limited to the minimum necessary for the specified purpose, and that the data should be obtained by lawful and fair means, with the consent of the data subject. Collection limitation reduces the attack surface for a customer's private information, as it reduces the amount and scope of the data that is exposed to potential threats, and ensures that the data is collected in a legitimate and transparent manner. Obfuscation, authentication, and data masking are not examples of minimizing the attack surface, but rather examples of protecting the data that is already collected. Obfuscation is a technique of obscuring or hiding the meaning or intent of the data, such as by using encryption, hashing, or encoding. Authentication is a process of verifying the identity or credentials of a user or a system that requests access to the data. Data masking is a technique of replacing or modifying the sensitive data with fictitious or anonymized data, such as by using pseudonymization, tokenization, or generalization.

NEW QUESTION: 604
IT 技術人員懷疑提供與核心交換器連接的上行鏈路之一出現故障。技術人員應使用下列哪些命令列工具來決定事件發生的位置？
A. nslookup
B. 顯示配置
C. 網路統計
D. 顯示介面
E. 顯示計數器
Answer: D (LEAVE A REPLY)
The "show interface" command is used to diagnose the status of an individual port or interface on a network device, such as a switch or router. It provides detailed information about the operational status, errors, and other relevant statistics that can help in identifying issues like a break in connectivity.

NEW QUESTION: 605

在設計新的網際網路語音協定 (VoIP) 網路時，組織最關心的是如何防止未經授權的使用者存取VoIP 網路。下列哪一項措施最有助於保護 VoIP 網路？

A. 傳輸層安全協定 (TLS)

B. 802.1x

C. 802.119

D. Web應用程式防火牆(WAF)

Answer: B (LEAVE A REPLY)

802.1x is the standard that will best help secure the VoIP network from unauthorized users. 802.1x is a protocol that provides port-based network access control, which means that it controls the access to a network port based on the authentication and authorization of the device or the user that is trying to connect to the port. 802.1x can be used to secure the VoIP network by preventing unauthorized devices or users from accessing the network ports that are used for VoIP communication, such as the ports on the switches, routers, or phones. 802.1x can also prevent unauthorized devices or users from accessing the network resources or services that are available through the VoIP network, such as voice mail, call forwarding, or conferencing. 802.1x can also prevent unauthorized devices or users from eavesdropping, intercepting, or modifying the VoIP traffic, by encrypting the communication between the devices and the network ports.

NEW QUESTION: 606

資料遺失防護 (DLP) 計畫中應考慮的第一步是什麼？

A. 組態管理 (CM)

B. 資訊權限管理 (IRM)

C. 策略創建

D. 資料分類

Answer: D (LEAVE A REPLY)

The first step that should be considered in a data loss prevention (DLP) program is data classification. Data loss prevention (DLP) is a type of process that involves identifying, monitoring, and protecting the data or the information on a system or a network, or on an organization or a business, using various methods, such as policies, rules, or tools, to prevent or mitigate the data or the information from being lost, leaked, or stolen by unauthorized parties, such as hackers, insiders, or competitors. DLP can provide various benefits, such as enhancing the security, compliance, or reputation of the system or the network, or of the organization or the business, and ensuring the confidentiality, integrity, or availability of the data or the information.

DLP can be implemented or performed by various steps or phases, such as:

Data classification: The step or the phase that involves defining, assigning, and labeling the data or the information on a system or a network, or on an organization or a business, using various criteria, categories, or levels, such as public, private, or confidential, to indicate or reflect the value, sensitivity, or importance of the data or the information, and to determine or guide the handling or the management of the data or the information.

Data discovery: The step or the phase that involves locating, identifying, and inventorying the data or the information on a system or a network, or on an organization or a business, using various methods,

such as scanning, mapping, or indexing, to understand or analyze the source, type, or content of the data or the information, and to assess or evaluate the risk or the exposure of the data or the information.
Data monitoring: The step or the phase that involves observing, tracking, and recording the data or the information on a system or a network, or on an organization or a business, using various sources, such as logs, alerts, or reports, to measure or evaluate the usage, activity, or behavior of the data or the information, and to detect or prevent the data or the information from being lost, leaked, or stolen.
Data protection: The step or the phase that involves applying or enforcing the policies, rules, or tools to the data or the information on a system or a network, or on an organization or a business, using various techniques, such as encryption, masking, or blocking, to prevent or mitigate the data or the information from being lost, leaked, or stolen, and to achieve or maintain the security, compliance, or reputation of the system or the network, or of the organization or the business.
Data classification is the first step that should be considered in a DLP program, as it can provide the foundation or the basis for the other steps or phases of the DLP program, and as it can enable or facilitate the identification, monitoring, and protection of the data or the information.

NEW QUESTION: 607
下列哪一個管理流程僅分配使用者完成任務、變更預設使用者密碼、設定伺服器擷取防毒更新所需的服務？
A. 合規性
B. 配置
C. 身份
D. 補丁
Answer: B (LEAVE A REPLY)
Configuration is the process of setting up and maintaining the parameters, settings, and options of a system or network to ensure its optimal performance and security. Configuration management is the process of controlling and documenting the changes made to the configuration of a system or network. Configuration management can help to allot only those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates. These actions can help to enhance the security, functionality, and efficiency of the system or network, as well as to prevent unauthorized or unnecessary access or use of the system or network resources. Compliance, identity, or patch are not the best management processes to allot only those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates, as they are more related to the audit, access control, or vulnerability management aspects of security.

NEW QUESTION: 608
當發現工業控制 (ICS) 軟體中的缺陷時，部署修補程式的最大障礙是什麼？
A. 許多 IG 系統的軟體不再由供應商維護。
B. 補償控制可能會影響 IG 效能。
C. 在 IG 中測試補丁可能需要比組織可以承諾的資源更多的資源。

D. 供應商需要驗證可操作性補丁。

Answer: (SHOW ANSWER)

Industrial control systems (ICS) are critical for the operation of many sectors such as energy, transportation, manufacturing, and water. Patching ICS software is a challenging task because it may require extensive testing, validation, and coordination to ensure that the patch does not introduce new vulnerabilities, affect the functionality, performance, or availability of the system, or cause any adverse impacts on the physical processes or safety. Testing a patch in an ICS may require more resources than the organization can commit, such as time, personnel, equipment, or budget. Therefore, this is the greatest impediment to deploying a patch for ICS software.

NEW QUESTION: 609

當涉及桌上型電腦時，保護證據鏈的第一個行動應該是什麼？

A. 將電腦帶到法醫實驗室

B. 製作硬碟的副本

C. 開始記錄

D. 關閉計算機

Answer: B (LEAVE A REPLY)

Making a copy of the hard drive should be the first action to protect the chain of evidence when a desktop computer is involved. A chain of evidence, also known as a chain of custody, is a process that documents and preserves the integrity and authenticity of the evidence collected from a crime scene, such as a desktop computer. A chain of evidence should include information such as:

The identity and role of the person who collected, handled, or transferred the evidence The date and time of the collection, handling, or transfer of the evidence The location and condition of the evidence The method and tool used to collect, handle, or transfer the evidence The signature or seal of the person who collected, handled, or transferred the evidence Making a copy of the hard drive should be the first action to protect the chain of evidence when a desktop computer is involved, because it can ensure that the original hard drive is not altered, damaged, or destroyed during the forensic analysis, and that the copy can be used as a reliable and admissible source of evidence. Making a copy of the hard drive should also involve using a write blocker, which is a device or a software that prevents any modification or deletion of the data on the hard drive, and generating a hash value, which is a unique and fixed identifier that can verify the integrity and consistency of the data on the hard drive.

NEW QUESTION: 610

通常使用什麼術語來描述儲存在組態管理資料庫 (CMDB) 中的硬體和軟體資口？

A. 配置元素

B. 資口暫存器

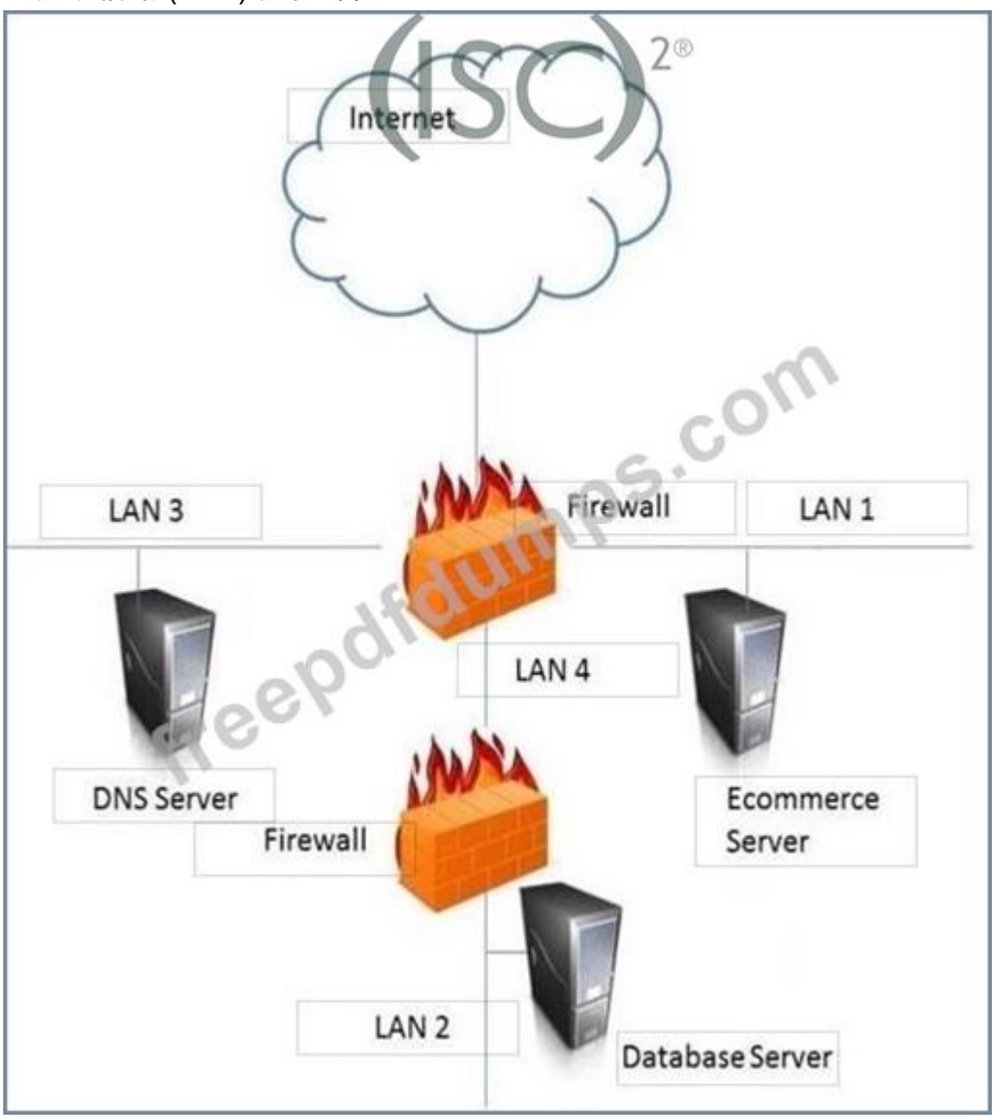
C. 分類帳項目

D. 設定項

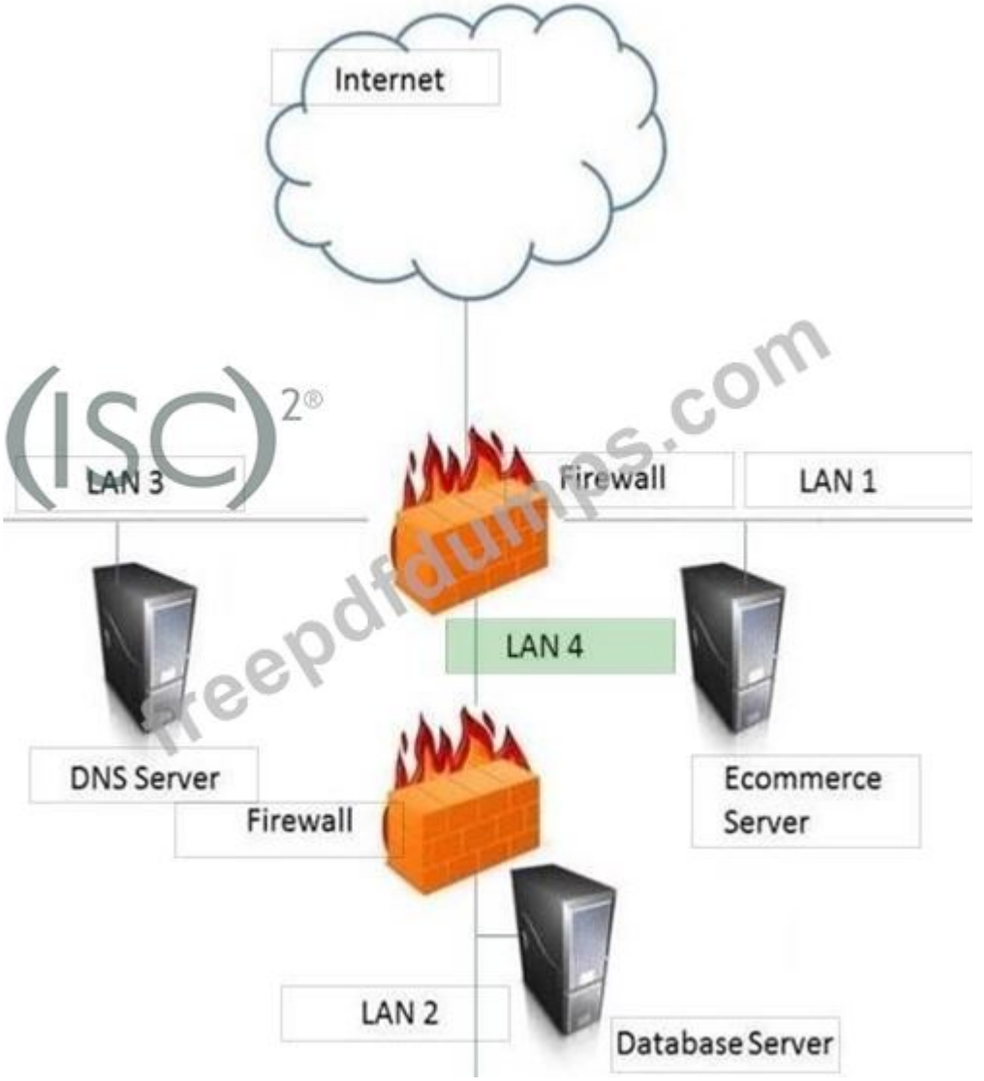
Answer: D (LEAVE A REPLY)

A configuration item is a term commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB). A configuration item is an identifiable and manageable component of a system or service that has a defined lifecycle and configuration.
A CMDB is a repository that contains information about the configuration items and their relationships.
A configuration element, an asset register, and a ledger item are not terms that are used to describe hardware and software assets in a CMDB.

NEW QUESTION: 611
熱點問題
在下面的網路設計中，部署無線存取點(WAP) 為承包商提供網際網路和授權企業服務存取權限的最安全的區域網路 (LAN) 段在哪裡？



Answer:



freepdfdumps.com

NEW QUESTION: 612
以下哪□最能描述“出口点 API 安全□□管理 (ASPM)”的目的？
A. 管理□ API 服□器的物理□□
B. 持□□□、清点和□估□□API(包括未□□的或“影子”API)的安全状况，以便在□□配置和漏洞被利用之前□□它□。
C. □□用于生成 API 文档的工具
D. 用于跟踪 API 使用成本的□□工具
Answer: B (LEAVE A REPLY)
API Security Posture Management continuously discovers and inventories an organization's APIs-including undocumented "shadow" or "zombie" APIs that may not be tracked through normal governance processes-and assesses their configuration and exposure for security weaknesses, addressing the growing risk surface created by the proliferation of APIs across modern application architectures.

NEW QUESTION: 613
在拆除、修理或更換任何物品之前，應在災難現場執行下列哪項操作？

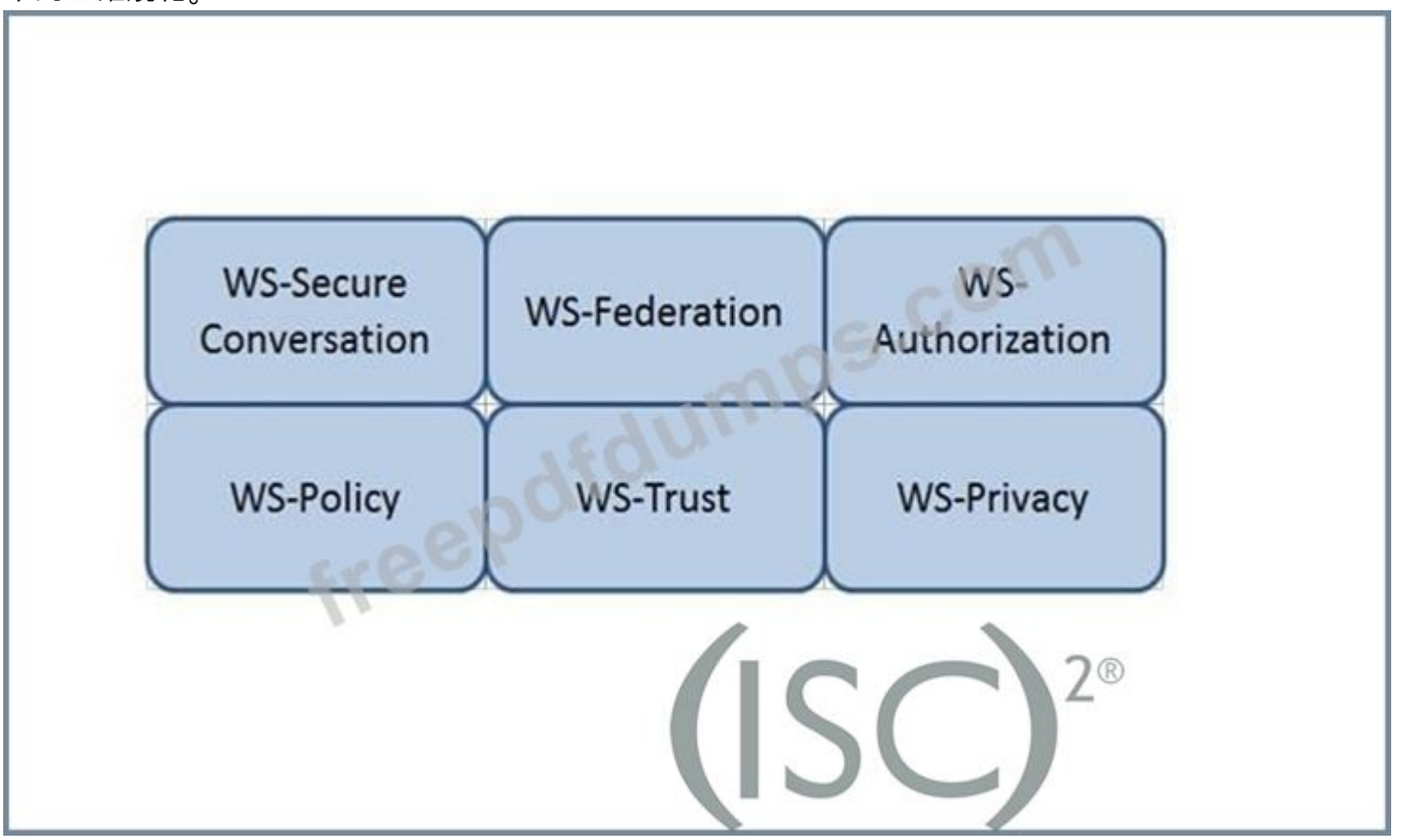
A. 拍攝損壞狀況的照片
B. 通知所有董事會
C. 依照溝通計畫與媒體溝通
D. 派遣人員到災難復原（DR）站點
Answer: A (LEAVE A REPLY)
The action that should be done at a disaster site before any item is removed, repaired, or replaced is to take photos of the damage. Taking photos of the damage is a part of the evidence preservation and documentation process, which is the process that involves collecting, preserving, and documenting the evidence of the disaster, such as the cause, the extent, the impact, or the timeline of the disaster. Taking photos of the damage can help to provide a visual and accurate record of the disaster site, and to support the investigation, analysis, and recovery of the disaster. Taking photos of the damage can also help to facilitate the communication, reporting, and decision making of the disaster, and to comply with the legal, regulatory, or contractual obligations of the disaster.

NEW QUESTION: 614
安全內容自動化協定 (SCAP) 規範的哪個元件包含估計自動漏洞評估所識別漏洞的嚴重性所需的資料？
A. 常見漏洞和暴露 (CVE)
B. 通用漏洞評分系統 (CVSS)
C. 資產報告格式 (ARF)
D. 開放漏洞和評估語言 (OVAL)
Answer: (SHOW ANSWER)
The component of the Security Content Automation Protocol (SCAP) specification that contains the data required to estimate the severity of vulnerabilities identified by automated vulnerability assessments is the Common Vulnerability Scoring System (CVSS). CVSS is a framework that provides a standardized and objective way to measure and communicate the characteristics and impacts of vulnerabilities. CVSS consists of three metric groups: base, temporal, and environmental. The base metric group captures the intrinsic and fundamental properties of a vulnerability that are constant over time and across user environments. The temporal metric group captures the characteristics of a vulnerability that change over time, such as the availability and effectiveness of exploits, patches, and workarounds. The environmental metric group captures the characteristics of a vulnerability that are relevant and unique to a user's environment, such as the configuration and importance of the affected system. Each metric group has a set of metrics that are assigned values based on the vulnerability's attributes. The values are then combined using a formula to produce a numerical score that ranges from 0 to 10, where
0 means no impact and 10 means critical impact. The score can also be translated into a qualitative rating that ranges from none to low, medium, high, and critical. CVSS provides a consistent and comprehensive way to estimate the severity of vulnerabilities and prioritize their remediation.

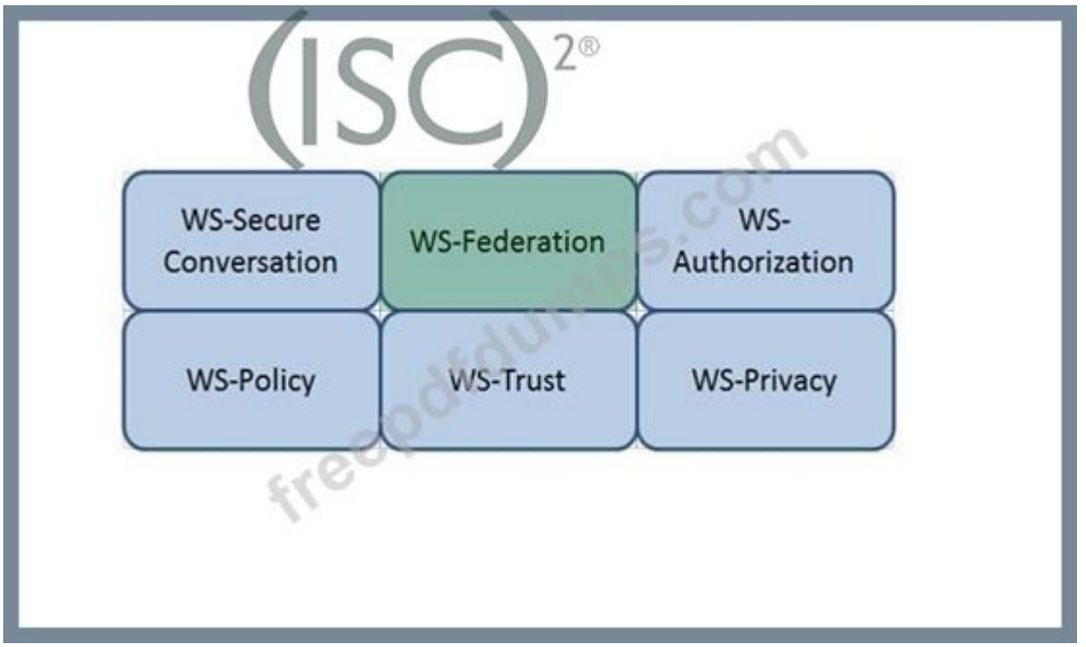
NEW QUESTION: 615
驗證 Web 會話管理需要存取下列哪一項？
A. 日誌時間戳

B. 即時會話流量
C. 會話狀態變數
D. 測試口本
Answer: C (LEAVE A REPLY)
Access to session state variables is required to validate web session management. Web session management is the process of maintaining the state and information of a user across multiple requests and interactions with a web application. Web session management relies on session state variables, which are data elements that store the user's preferences, settings, authentication status, and other relevant information for the duration of the session. Session state variables can be stored on the client side (such as cookies or local storage) or on the server side (such as databases or files). To validate web session management, it is necessary to access the session state variables and verify that they are properly generated, maintained, and destroyed by the web application. This can help to ensure the security, functionality, and performance of the web application and the user experience.

NEW QUESTION: 616
熱點問題
哪種 Web 服務安全性 (WS-Security) 規範能口在多個不同的環境中維護單一的已認證身分？請點選下圖中的正確規範。



Answer:



Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 617
應用程式開發人員收到安全團隊返回的報告，顯示他們的自動化工具能□成功地將意外資料輸入組織的客□服務門□，導致網站崩潰 這是哪種類型測試的範例？
A. 不起作用
B. 正數
C. 效能
D. 負數
Answer: D (LEAVE A REPLY)
Negative testing is an example of the type of testing that the security team performed on the organization's customer service portal. Negative testing is a technique that tests the system or the application with invalid, unexpected, or erroneous inputs or data, such as alphabets in a numeric field, special characters in a text field, or null values in a mandatory field. Negative testing can help to evaluate the robustness, stability, and error handling of the system or the application, and to identify and fix the bugs, flaws, or vulnerabilities that may cause the system or the application to crash, malfunction, or behave unpredictably.

NEW QUESTION: 618
下列哪一項是使用組態管理的主要原因？

A. 提供集中管理
B. 減少更改次數
C. 減少升級過程中的錯誤
D. 提供安全控制的一致性
Answer: D (LEAVE A REPLY)
The main reason for using configuration management is to provide consistency in security controls. Configuration management is the process of identifying, documenting, controlling, and verifying the characteristics and settings of the hardware, software, data, and network components of a system. Configuration management helps to ensure that the system is configured and maintained according to the security policies, standards, and baselines, and that any changes to the system are authorized, recorded, and tracked. Configuration management also helps to prevent or detect unauthorized or unintended changes to the system, which may introduce vulnerabilities, errors, or inconsistencies. Configuration management does not necessarily provide centralized administration, although it may involve some centralized tools or processes to facilitate the configuration management activities. Configuration management does not aim to reduce the number of changes, although it may help to prioritize, schedule, and coordinate the changes to minimize the impact and disruption to the system. Configuration management does not aim to reduce errors during upgrades, although it may help to test, validate, and verify the upgrades before implementing them on the system.

NEW QUESTION: 619
災難復原計畫 (DRIP) 的復原策略必須與下列哪一項保持一致？
A. 硬體和軟體相容性問題
B. 應用程式的關鍵和停機容忍度
C. 預算限制與要求
D. 成本/效益分析與業務目標
Answer: D (LEAVE A REPLY)
Recovery strategies of a Disaster Recovery planning (DRP) must be aligned with the cost/benefit analysis and business objectives. A DRP is a part of a BCP/DRP that focuses on restoring the normal operation of the organization's IT systems and infrastructure after a disruption or disaster.
A DRP should include various components, such as:
Risk assessment: a process that identifies and evaluates the potential threats and vulnerabilities that might affect the IT systems and infrastructure, and estimates the likelihood and impact of a disruption or disaster Recovery objectives: a process that defines and quantifies the acceptable levels of recovery for the IT systems and infrastructure, such as the recovery point objective (RPO), which is the maximum amount of data loss that can be tolerated, and the recovery time objective (RTO), which is the maximum amount of downtime that can be tolerated Recovery strategies: a process that selects and implements the appropriate methods and resources to recover the IT systems and infrastructure, such as backup, replication, redundancy, or failover DRP document: a document that outlines and details the scope, purpose, and features of the DRP, such as the roles and responsibilities, the recovery procedures, and the contact information Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the DRP, and educates and trains the

relevant stakeholders, such as the IT staff, the management, and the users, on the DRP and their roles and responsibilities Maintenance and review: a process that monitors and updates the DRP, and addresses any changes or issues that might affect the DRP, such as the IT requirements, the threat landscape, or the feedback and lessons learned Recovery strategies of a DRP must be aligned with the cost/benefit analysis and business objectives, because it can ensure that the DRP is feasible and suitable, and that it can achieve the desired outcomes and objectives in a cost-effective and efficient manner. A cost/benefit analysis is a technique that compares the costs and benefits of different recovery strategies, and determines the optimal one that provides the best value for money. A business objective is a goal or a target that the organization wants to achieve through its IT systems and infrastructure, such as increasing the productivity, profitability, or customer satisfaction. A recovery strategy that is aligned with the cost/benefit analysis and business objectives can help to:
Optimize the use and allocation of the IT resources and funds for the recovery Minimize the negative impacts and risks of a disruption or disaster on the IT systems and infrastructure Maximize the positive outcomes and benefits of the recovery for the IT systems and infrastructure Support and enable the achievement of the organizational goals and targets through the IT systems and infrastructure

NEW QUESTION: 620
在防火牆或路由器上實施下列哪一項措施可以有效隱藏網路位址，防止其暴露於外部？
A. 網路位址轉換(NAT)
B. 應用程式代理
C. 路由資訊協定(RIP)版本 2
D. 位址掩碼
Answer: A (LEAVE A REPLY)
Network Address Translation (NAT) is the most effective method for obscuring network addresses from external exposure when implemented on a firewall or router. NAT is a technique that allows a device, such as a firewall or a router, to modify the source or destination IP address of a packet as it passes through the device. NAT can be used to hide the internal IP addresses of a network from the external network, such as the internet, by replacing them with a public IP address. This can enhance the security and privacy of the network, as well as conserve the limited IPv4 address space. Application proxy, RIP version 2, and address masking are not methods for obscuring network addresses from external exposure, as they are either related to different functions or not implemented on a firewall or router.

NEW QUESTION: 621
一項違規調口發現，一個網站被開源元件利用。可以防止這種破壞的過程的第一步是什麼？
A. 應用程式白名單
B. Web 應用程式防火牆 (WAF)
C. 漏洞修復
D. 軟體清單
Answer: D (LEAVE A REPLY)

The breach occurred due to an exploited open-source component. The FIRST step to prevent this is D. Software inventory, and here's why:
CISSP Domain Alignment:
Domain 2 (Asset Security) and Domain 8 (Software Development Security) emphasize maintaining a software inventory to track all components (including open-source libraries).
Without knowing what software is in use, vulnerabilities cannot be identified or managed.

NEW QUESTION: 622
在實施安全無線網路時，下列哪一項支援單一用口端端點的身份驗證和授權？
A. 臨時金鑰完整性協定 (TKIP)
B. Wi-Fi 保護存取 (WPA) 預先共用金鑰 (PSK)
C. Wi-Fi 保護存取 2 (WPA2) 企業版
D. 使用密碼區塊連結訊息驗證代碼協定 (CCMP) 的計數器模式
Answer: C (LEAVE A REPLY)
When implementing a secure wireless network, the option that supports authentication and authorization for individual client endpoints is Wi-Fi Protected Access 2 (WPA2) Enterprise.
WPA2 is a security protocol that provides encryption and authentication for wireless networks, based on the IEEE 802.11i standard. WPA2 has two modes: Personal and Enterprise. WPA2 Personal uses a Pre- Shared Key (PSK) that is shared among all the devices on the network, and does not require a separate authentication server. WPA2 Enterprise uses an Extensible Authentication Protocol (EAP) that authenticates each device individually, using a username and password or a certificate, and requires a Remote Authentication Dial-In User Service (RADIUS) server or another authentication server. WPA2 Enterprise provides more security and granularity than WPA2 Personal, as it can support different levels of access and permissions for different users or groups, and can prevent unauthorized or compromised devices from joining the network.
Temporal Key Integrity Protocol (TKIP), Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK), and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) are not the options that support authentication and authorization for individual client endpoints, as they are related to the encryption or integrity of the wireless data, not the identity or access of the wireless devices.

NEW QUESTION: 623
就所使用的屬性而言，下列哪些因素應被視為基於屬性的存取控制(ABAC) 的特徵？
A. 強制存取控制 (MAC) 和自主存取控制 (DAC)
B. 自主存取控制 (DAC) 和存取控制清單 (ACL)
C. 基於角色的存取控制 (RBAC) 和強制存取控制 (MAC)
D. 基於角色的存取控制 (RBAC) 和存取控制清單 (ACL)
Answer: (SHOW ANSWER)
RBAC Integration: Attribute-Based Access Control (ABAC) can be integrated with RBAC. User roles (from RBAC) can become one of the many attributes considered by an ABAC system when making access decisions.

ACL Refinement: ABAC can leverage and refine the use of ACLs. With ABAC, permissions on an ACL can be granted or denied based on various attributes rather than solely on user identities or roles.

NEW QUESTION: 624
經過全面分析，發現攻擊者透過安全通訊端(SSL) 虛擬私人網路 (VPN) 閘道入侵網路。攻擊者猜測使用者名稱並暴力破解密碼，從而獲得存取權限
下列哪一項措施最能緩解這個問題？
A. 為 VPN 實現強密碼認證
B. 將 VPN 與集中式憑證儲存集成
C. 實現網際網路協定安全(IPSec)客口端
D. 使用雙重認證機制
Answer: D (LEAVE A REPLY)
The best way to mitigate the issue of a perpetrator compromising a network by gaining access to the network through an SSL VPN gateway by guessing a username and brute forcing the password is to use two-factor authentication mechanisms. Two-factor authentication is a method of verifying the identity of a user or device by requiring two different types of factors, such as something the user knows (e.g., password, PIN, etc.), something the user has (e.g., token, smart card, etc.), or something the user is (e.g., biometric, fingerprint, etc.). Two-factor authentication can enhance the security of the network access by making it harder for attackers to impersonate or compromise the legitimate users or devices. If the perpetrator only knows the username and password, they will not be able to access the network without the second factor, such as a token or a biometric

NEW QUESTION: 625
以下哪口最能描述数据中心或云口境中“出口点微隔离”的目的？
A. 在整个扁平网口中口用口一、口一的安全策略
B. 将网口划分口非常口粒度的网段——通常口化到口个工作口口或口用程序口口——并使用口格且独立口行的安全策略来控制网段之口的流量。
C. 口了口化操作，将所有工作口口整合到口个未分段的网口中。
D. 口所有内部工作口口分配公网IP地址
Answer: (SHOW ANSWER)
Micro-segmentation divides a network into very granular, often workload- or application-level segments, applying strict and independently enforced security policies to control traffic flow between them. This significantly limits an attacker's ability to move laterally within the environment even after gaining initial access to one segment, compared to traditional, more coarsely segmented network architectures.

NEW QUESTION: 626
供應鏈營運中口得信賴的軟體有哪些面向？
A. 功能性、安全性、可靠性、完整性和準確性
B. 機密性、完整性、可用性、真實性和所有權
C. 安全性、可靠性、可用性、彈性和保障

D. 可修復性、安全性、可升級性、功能性和準確性

Answer: (SHOW ANSWER)

Trustworthy software in supply chain operations requires that the software possess key characteristics such as safety, reliability, availability, resilience, and security. Safety ensures that the software does not harm people or the environment. Reliability ensures that the software works as intended and does not fail prematurely. Availability ensures that the software is available when needed. Resilience ensures that the software can withstand and recover from disruptions. Security ensures that the software is protected from unauthorized access, modification, or destruction.

NEW QUESTION: 627

攻擊者侵入了原始碼管理系統，可以下載但無法修改程式碼。代碼盜竊的下列哪些方面具有最高的安全影響？

A. 攻擊者可以公開分享在被竊代碼中發現的機密註解。

B. 競爭對手可能能□透過□看被盜代碼來竊取組織的想法。

C. 競爭對手可以使用竊取的程式碼來執行自己的組織網站副本。

D. 被盜代碼中硬編碼的管理憑證或金鑰可用於存取敏感資料。

Answer: D (LEAVE A REPLY)

Hard-coded credentials or keys in the source code represent a critical security vulnerability. If an attacker gains access to the source code and finds such sensitive information, they could potentially use it to gain unauthorized access to databases, servers, or other critical systems, leading to a breach of sensitive data or systems.

While other options (like sharing confidential comments, stealing ideas, or running a competitor's copy of the website) can have negative business and reputational consequences, they do not pose as immediate and severe a threat to the security of sensitive systems and data as the potential use of hard-coded credentials.

NEW QUESTION: 628

為了確保遵守一般資料保護規範 (GDPR)，幫助台經理在選擇軟體即服務(SaaS) 解決方案之前應與組織中的誰進行協商？

A. 資料保護官 (DPO)

B. 資料中心經理

C. 資料庫管理員 (DBA)

D. 資料擁有者

Answer: A (LEAVE A REPLY)

NEW QUESTION: 629

以下哪□最能描述“非□称”加密相□于□称加密在密□分□方面的主要□□？

A. 加密大量数据速度更快

B. 由于每一方都□有自己的公□/私□□，因此无需事先安全地共享密□。

C. 它使用的密□比□称加密更短。

D. 无需任何密口管理

Answer: B (LEAVE A REPLY)

Asymmetric encryption solves the key distribution problem inherent in symmetric encryption: each party generates their own key pair (public and private), and the public key can be freely shared without compromising security, eliminating the need to transmit a shared secret key over a potentially insecure channel.

NEW QUESTION: 630

下列哪一項是最適合銷毀包含 高」安全類別資料的磁碟式硬碟 (HDD) 的技術？

A. 鑽穿設備和盤片。

B. 機械性粉碎整個硬碟。

C. 拆下控制電子設備。

D. HP iProcess 透過消磁設備處理 HDD。

Answer: B (LEAVE A REPLY)

Mechanically shredding the entire HDD is the most appropriate technique for destroying magnetic platter style hard disk drives containing data with a "HIGH" security categorization. Mechanical shredding is a process that uses a powerful machine to cut, tear, or crush the HDD into small pieces, making it impossible to recover any data from the platters or the components. Mechanical shredding is the most appropriate technique for destroying HDDs with high security data, because it can:
Ensure the complete and irreversible destruction of the HDD and the data, regardless of the type, size, or condition of the HDD, and without requiring any prior preparation or disassembly of the HDD.
Provide a high level of assurance and confidence that the HDD and the data are destroyed beyond any possibility of recovery, even by advanced forensic techniques or specialized equipment.
Comply with the industry standards and the best practices for the secure disposal of HDDs and the data, such as the National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, or the Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual.

NEW QUESTION: 631

當使用安全多用途互聯網郵件擴充 (S/MIME) 時，安全專業人員應確保用口端支援哪種輔助數位簽章演算法？

A. 三重資料加密標準 (3DES)

B. 進階加密標準 (AES)

C. 數位簽章演算法 DSA）

D. 裡維斯特沙米爾阿迪曼 (RSA)

Answer: D (LEAVE A REPLY)

S/MIME is a standard for secure email that uses asymmetric encryption and digital signatures. S/MIME supports several algorithms for digital signatures, but the most common ones are RSA and DSA. RSA is a more versatile algorithm that can be used for both encryption and digital signatures, while DSA is designed only for digital signatures. RSA is also more widely supported by email clients

and servers than DSA. Therefore, a security professional should ensure that clients support RSA as a secondary algorithm for digital signatures when S/MIME is used, in case the primary algorithm is not available or compatible.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 632
下列哪一項是組織的安全專業人員在根據業界標準定義網路安全計畫時執行的第一步？
A. 將組織目前的安全實踐映射到行業標準和框架。
B. 定義組織有關安全和風險緩解的目標。
C. 從安全最佳實務中進行選擇。
D. 回顧過去的安全評估。
Answer: (SHOW ANSWER)
The first step an organization's security professional performs when defining a cybersecurity program based on industry standards is to define the organization's objectives regarding security and risk mitigation. A cybersecurity program is a set of policies, procedures, and practices that aim to protect the organization's information assets and systems from cyber threats and attacks.
A cybersecurity program should be based on industry standards and frameworks, such as ISO/IEC 27001, NIST SP 800-53, or COBIT, that provide best practices and guidelines for establishing and maintaining an effective and efficient cybersecurity program. The first step in defining a cybersecurity program based on industry standards is to define the organization's objectives regarding security and risk mitigation, which are the goals or outcomes that the organization wants to achieve or accomplish through the cybersecurity program. The objectives should be aligned with the organization's mission, vision, values, and strategy, and they should reflect the organization's risk appetite, risk tolerance, and risk management approach. The objectives should also be specific, measurable, achievable, relevant, and time-bound (SMART), and they should be communicated and agreed upon by the relevant stakeholders, such as the management, the staff, or the customers.

NEW QUESTION: 633
為什麼所有權認證比知識認證更強？
A. 更容易更改。
B. 可以隨身攜帶。
C. 複製比較困難。
D. 控制更簡單。

Answer: (SHOW ANSWER)
Authentication by ownership is stronger than authentication by knowledge because it is more difficult to duplicate. Authentication by ownership is a type of authentication that relies on something that the user possesses, such as a smart card, a token, or a biometric feature.
Authentication by knowledge is a type of authentication that relies on something that the user knows, such as a password, a PIN, or a security question. Authentication by ownership is more difficult to duplicate than authentication by knowledge, as it requires physical access, specialized equipment, or sophisticated techniques to copy or forge the authentication factor. Authentication by knowledge is easier to duplicate than authentication by ownership, as it may be guessed, cracked, or stolen by various methods, such as brute force, social engineering, or phishing.
Authentication by ownership is not necessarily easier to change, simpler to control, or more convenient to keep on the user's person than authentication by knowledge, as these factors may depend on the specific implementation and context of the authentication system.

NEW QUESTION: 634
以下哪□最能描述□用于云文件共享服□的“出□点数据□失防□ (DLP) 策略”的目的？
A. 完全阻止□云文件共享服□的所有□□
B. □□和控制敏感数据向云服□的共享或上□，防止未□授□的泄露，同□允□合法的商□用途
C. 加密存□在□端□□上的所有本地文件
D. 用于管理云□□的用□密□重置
Answer: B (LEAVE A REPLY)
DLP policies applied to cloud file-sharing services inspect content being uploaded or shared, applying rules to detect sensitive data (such as PII, financial data, or intellectual property) and blocking, quarantining, or alerting on policy violations, balancing the need for legitimate collaboration with the requirement to prevent unauthorized exposure of sensitive information.

NEW QUESTION: 635
下列哪一種類型的主機應在非軍事區 (DMZ) 中運作？
A. 旨在提供對公共資源的有限存取的主機
B. 可以提供公眾有用資訊的資料庫伺服器
C. 儲存人口統計資訊等不重要資料的主機
D. 包含組織資料的檔案伺服器
Answer: (SHOW ANSWER)
A demilitarized zone (DMZ) is a network segment that is separated from both the internal and external networks by firewalls. The purpose of a DMZ is to provide limited access to public resources, such as web servers, email servers, or DNS servers, while protecting the internal network from unauthorized access. A DMZ should not contain database servers, file servers, or hosts that store sensitive or unimportant data, as these could be compromised by attackers who gain access to the DMZ.

NEW QUESTION: 636
下列哪一項對於成功的審計計劃最為重要？

A. 定義要執行的稽核範圍
B. 確定要實施的安全控制
C. 與系統擁有者合作開發新控件
D. 取得不合規系統的證據
Answer: (SHOW ANSWER)
An audit is an independent and objective examination of an organization's activities, systems, processes, or controls to evaluate their adequacy, effectiveness, efficiency, and compliance with applicable standards, policies, laws, or regulations. An audit plan is a document that outlines the objectives, scope, methodology, criteria, schedule, and resources of an audit. The most crucial element of a successful audit plan is defining the scope of the audit to be performed, which is the extent and boundaries of the audit, such as the subject matter, the time period, the locations, the departments, the functions, the systems, or the processes to be audited. The scope of the audit determines what will be included or excluded from the audit, and it helps to ensure that the audit objectives are met and the audit resources are used efficiently and effectively. Identifying the security controls to be implemented, working with the system owner on new controls, and acquiring evidence of systems that are not compliant are all important tasks in an audit, but they are not the most crucial for a successful audit plan, as they depend on the scope of the audit to be defined first.

NEW QUESTION: 637
下列哪一項是資訊所有者的責任？
A. 確保使用者和人員完成存取資訊系統 (IS) 所需的安全培訓
B. 定義對資訊系統 (IS) 的正確訪問，包括特權或存取權限
C. 管理常見安全控制的識別、實施與評估
D. 確保資訊系統 (IS) 根據商定的安全要求運行
Answer: B (LEAVE A REPLY)
One of the responsibilities of the information owner is to define proper access to the Information System (IS), including privileges or access rights. This involves determining who can access the data, what they can do with the data, and under what conditions they can access the data. The information owner must also approve or deny the access requests and periodically review the access rights. Ensuring that users and personnel complete the required security training, managing the common security controls, and ensuring the IS is operated according to the security requirements are not the responsibilities of the information owner, but they may involve the information owner's collaboration or consultation.

NEW QUESTION: 638
下列哪一項是保護自動櫃員機(ATM)免遭盜刷的實體安全控制措施？
A. 防口改
B. 安全讀卡機
C. 射頻(RF)掃描儀
D. 入侵防禦系統(IPS)
Answer: B (LEAVE A REPLY)

A secure card reader is a physical security control that protects ATM from skimming, which is a type of fraud where a device is attached to the card slot of an ATM to capture the data from the magnetic stripe of the card. A secure card reader can prevent skimming by encrypting the data at the point of entry, making it unreadable by the skimming device. Anti-tampering, RF scanner, and IPS are not physical security controls that protect ATM from skimming, as they do not prevent the capture of the card data by the skimming device.

NEW QUESTION: 639
某個組織正在考慮與第三方雲端服務供應商合作。該組織將僅提供數據，第三方供應商將提供安全控制。下列哪一項最能描述此服務？
A. 平台即服務 (PaaS)
B. 基礎設施即服務 (IaaS)
C. 軟體即服務 (SaaS)
D. 一切即服務 (XaaS)
Answer: C (LEAVE A REPLY)
SaaS is a service offering that provides the software or the application that is hosted and managed by the service provider or the vendor, and that is accessed and used by the client or the customer over the network or the internet, such as the web browser, the email, or the office suite.
SaaS best describes the scenario where the organization will only be providing the data and the third-party supplier will be providing the security controls, because it can:
Allow the organization to focus on the core business functions or processes, and to reduce the cost and the complexity of the software or the application development, deployment, maintenance, or support, by outsourcing the software or the application to the third-party supplier.
Allow the third-party supplier to take the responsibility and the accountability for the security controls of the software or the application, such as the authentication, the authorization, the encryption, or the backup, and to ensure the confidentiality, the integrity, and the availability of the software or the application and the data.
Allow the organization to access and use the software or the application and the data from any system or device, and from any location or time, and to benefit from the scalability, the performance, and the functionality of the software or the application and the data.

NEW QUESTION: 640
下列哪一種類型的裝置可以提供口容過濾和威脅防護，並管理多個IPSec 網站到網站連線？
A. 三層交換機
B. VPN 頭端
C. 下一代防火牆
D. 代理伺服器
E. 入侵防禦
Answer: C (LEAVE A REPLY)
A next-generation firewall (NGFW) is a type of device that can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections. A NGFW can inspect and block

malicious or unwanted traffic based on application, user, or content level. A NGFW can also establish and maintain secure tunnels between different networks using IPSec, a protocol that encrypts and authenticates the data packets. A NGFW is the best option to provide the functionality of content filtering, threat protection, and IPSec site-to-site connections.

NEW QUESTION: 641
對組織的審核日誌進行徹底審口後發現，心懷不滿的網路管理員攔截了發給執行長(CEO) 的電子郵件，並在將其轉發給預期收件人之前對其進行了更改。最有可能發生什麼類型的攻擊？
A. 欺騙
B. 竊聽
C. 中間人
D. 拒口服務
Answer: (SHOW ANSWER)
The type of attack that has most likely occurred when a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient is a man-in-the-middle (MITM) attack. A MITM attack is a type of attack that involves an attacker intercepting, modifying, or redirecting the communication between two parties, without their knowledge or consent. The attacker can alter, delete, or inject data, or impersonate one of the parties, to achieve malicious goals, such as stealing information, compromising security, or disrupting service. A MITM attack can be performed on various types of networks or protocols, such as email, web, or wireless. Spoofing, eavesdropping, and denial of service are not the types of attack that have most likely occurred in this scenario, as they do not involve the modification or manipulation of the communication between the parties, but rather the falsification, observation, or prevention of the communication.

NEW QUESTION: 642
組織允許 ping 流量進出其網路。攻擊者在網路上安裝了一個程序，該程序使用ping 封包的有效負載部分將資料移入和移出網路。該組織經歷過什麼類型的攻擊？
A. 資料外洩
B. 未過濾的頻道
C. 資料發射
D. 隱蔽通道
Answer: D (LEAVE A REPLY)
The organization has experienced a covert channel attack, which is a technique of hiding or transferring data within a communication channel that is not intended for that purpose. In this case, the attacker has used the payload portion of the ping packet, which is normally used to carry diagnostic data, to move data into and out of the network. This way, the attacker can bypass the network security controls and avoid detection. Data leakage (A) is a general term for the unauthorized disclosure of sensitive or confidential data, which may or may not involve a covert channel. Unfiltered channel (B) is a term for a communication channel that does not have any security mechanisms or filters applied to it, which may allow unauthorized or malicious traffic to pass through. Data emanation is a term for the unintentional

radiation or emission of electromagnetic signals from electronic devices, which may reveal sensitive or confidential information to eavesdroppers.

NEW QUESTION: 643
以下哪□最能描述密□交□□□中的“完美前向保密(PFS)”？
A. 一种属性，确保□期私□泄露不会泄露用于加密先前通信的会□密□。
B. 一种生成永不□期密□的方法
C. 保□加密数据永□无法解密，即使是授□方也无法解密。
D. □称加密算法特有的属性
Answer: A (LEAVE A REPLY)
Perfect Forward Secrecy ensures that each session uses a unique, ephemeral key derived independently of the long-term private key, so that even if an attacker later compromises the long-term private key, they cannot use it to decrypt previously captured session traffic, since the ephemeral session keys were never derived from (and are not recoverable from) the long-term key.

NEW QUESTION: 644
以下哪□最能描述“□□□□性：□用□□流程策略？
A. 一种完全依□IT系□故障□移的策略
B. 一种策略，即在正常自□化系□不可用□，采用人工□通方法或替代方法(例如□□流程)来□持关□□□功能的运行，而不是□□依□于恢复技□系□本身。
C. 一种需要立即□止受影响□□□能的策略
D. □适用于制造企□的策略
Answer: (SHOW ANSWER)
Alternate business process strategies involve identifying manual workarounds or alternative methods-such as temporarily reverting to paper-based order processing-that allow a critical business function to continue operating, at least in a limited capacity, while normal automated systems are unavailable and being restored, complementing pure IT-focused disaster recovery strategies with broader business continuity planning.

NEW QUESTION: 645
在系統安全工程中，模組化的安全原則提供了什麼？
A. 函數的文檔
B. 獨立的函數與數據
C. 程式和資料的安全分發
D. 執行功能的最小存取權限
Answer: B (LEAVE A REPLY)
In systems security engineering, the security principle of modularity provides isolated functions and data. Modularity means dividing a system into well-defined logical units that have clear boundaries and interfaces. This helps to reduce complexity, improve maintainability, and enhance security. By isolating functions and data, modularity prevents unauthorized access, limits the impact of failures, and

facilitates testing and verification. Modularity also supports the principle of least privilege, which grants the minimum access required to perform a function.

NEW QUESTION: 646
在進行存取控制安全評估時，資料分析階段的哪個活動是主要環節？
A. 收集日誌和報告。
B. 提出解決審計異常情況的方案。
C. 對審計過程中收集的證據進行分類和識別
D. 對資料交易進行統計抽樣。
Answer: (SHOW ANSWER)
When conducting a security assessment of access controls, categorizing and identifying evidence gathered during the audit is an activity that is part of the data analysis phase. The data analysis phase is the stage of the security assessment process where the auditor examines and evaluates the data collected during the data gathering phase, and compares it with the predefined criteria, standards, and objectives. The data analysis phase involves categorizing and identifying the evidence gathered during the audit, such as logs, reports, records, interviews, observations, and tests, and determining whether they support or contradict the audit findings and conclusions.
Collecting logs and reports, presenting solutions to address audit exceptions, and conducting statistical sampling of data transactions are not activities that are part of the data analysis phase, although they may be involved in other phases of the security assessment process. Collecting logs and reports is an activity that is part of the data gathering phase, which is the stage where the auditor obtains and verifies the relevant information and evidence for the audit. Presenting solutions to address audit exceptions is an activity that is part of the reporting phase, which is the stage where the auditor communicates the audit results and recommendations to the stakeholders. Conducting statistical sampling of data transactions is an activity that is part of the planning phase, which is the stage where the auditor defines the scope, objectives, criteria, and methodology of the audit.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 647
在獲得對識別和存取管理 (IAM) 解決方案的支援時，下列哪一項是獲得的最佳指標？
A. 應用程式連線成功導致資料外洩
B. 連線失敗後復原系統的管理成本
C. 員工係統因實施錯誤限製而逾時
D. 支援密碼重設請求所需的服務台費用

Answer: (SHOW ANSWER)

Identify and Access Management (IAM) is the process of managing the identities and access rights of users and devices in an organization. IAM solutions can provide various benefits, such as improving security, compliance, productivity, and user experience. However, implementing an IAM solution may also require significant investment and resources, and therefore, it is important to obtain support from the stakeholders and decision-makers. One of the best metrics to obtain when gaining support for an IAM solution is the help desk costs required to support password reset requests. This metric can demonstrate the following advantages of an IAM solution:

Reducing the workload and expenses of the help desk staff, who often spend a large amount of time and money on handling password reset requests from users who forget or lose their passwords.

Enhancing the security and compliance of the organization, by reducing the risks of unauthorized access, identity theft, phishing, and credential compromise, which can result from weak or shared passwords, or passwords that are not changed frequently or securely.

Improving the productivity and user experience of the users, by enabling them to reset their own passwords quickly and easily, without having to contact the help desk or wait for a response. This can also reduce the downtime and frustration of the users, and increase their satisfaction and loyalty.

NEW QUESTION: 648

下列哪一項是最全面的業務連續性 (BC) 測試？

A. 全功能練習

B. 全桌面

C. 完全模擬

D. 完全中斷

Answer: D (LEAVE A REPLY)

The most comprehensive Business Continuity (BC) test is the full interruption test. A full interruption test is a type of BC test that involves shutting down the primary site or system and activating the alternate site or system, as if a real disaster has occurred. A full interruption test is the most realistic and effective way to evaluate the BC plan, as it tests the actual recovery capabilities and performance of the organization under a simulated disaster scenario. A full interruption test can measure the recovery time objective (RTO), recovery point objective (RPO), and other metrics of the BC plan, as well as identify any gaps, issues, or weaknesses in the plan.

A full interruption test can also test the communication, coordination, and documentation of the BC team, as well as the awareness, readiness, and resilience of the organization. However, a full interruption test is also the most risky and costly type of BC test, as it can disrupt the normal operations and services of the organization, cause potential loss of revenue or reputation, and expose the organization to legal or regulatory liabilities. Therefore, a full interruption test should be carefully planned, approved, and executed, with proper backup, contingency, and rollback measures in place. A full functional drill, a full table top, and a full simulation are not the most comprehensive BC tests. A full functional drill is a type of BC test that involves performing the actual recovery procedures and tasks at the alternate site or system, without shutting down the primary site or system. A full functional drill is less realistic and effective than a full interruption test, as it does not test the actual switch-over and

switch-back processes of the BC plan. A full table top is a type of BC test that involves discussing and reviewing the BC plan and procedures with the BC team and stakeholders, using a simulated disaster scenario. A full table top is less realistic and effective than a full interruption test, as it does not test the actual execution and performance of the BC plan. A full simulation is a type of BC test that involves simulating the recovery environment and activities at the alternate site or system, using a computer model or a virtual machine, without shutting down the primary site or system. A full simulation is less realistic and effective than a full interruption test, as it does not test the actual recovery capabilities and performance of the organization under a simulated disaster scenario.

NEW QUESTION: 649
在開放系統互連(OSI)模型中，哪一層負責透過通訊網路傳輸二進位資料？
A. 應用層
B. 物理層
C. 資料鏈結層
D. 網路層
Answer: B (LEAVE A REPLY)
In the Open System Interconnection (OSI) model, the layer that is responsible for the transmission of binary data over a communications network is the Physical Layer. The OSI model is a conceptual framework or a reference model that describes or defines how the different components or elements of a communications network interact or communicate with each other, using a layered or a modular approach. The OSI model consists of seven layers, each with a specific function or role, and each communicating or interfacing with the adjacent layers. The Physical Layer is the lowest or the first layer of the OSI model, and it is responsible for the transmission of binary data over a communications network, which means that it is responsible for converting or encoding the data or the information into electrical signals, optical signals, or radio waves, and sending or receiving them over the physical medium or the channel, such as the cable, the fiber, or the air. The Physical Layer is also responsible for defining or specifying the physical characteristics or the properties of the physical medium or the channel, such as the voltage, the frequency, the bandwidth, or the modulation.

NEW QUESTION: 650
以下哪种网□拓扑□构能□提供最高的容□能力，因□每个□点都与其他所有□点相□？
A. □□拓扑
B. □拓扑
C. 星形拓扑
D. 网格拓扑
Answer: D (LEAVE A REPLY)
In a full mesh topology, every device has a direct point-to-point connection to every other device, providing maximum redundancy and fault tolerance since failure of one link or node does not isolate the network, though it is costly and complex to implement at scale.

NEW QUESTION: 651

下列哪一項違反了身分和存取管理最佳實務？

A. 使用者帳□

B. 系統帳□

C. 通用帳□

D. 特權帳□

Answer: C (LEAVE A REPLY)

The type of accounts that violates identity and access management best practices is generic accounts. Generic accounts are accounts that are shared by multiple users or devices, and do not have a specific or unique identity associated with them. Generic accounts are often used for convenience, compatibility, or legacy reasons, but they pose a serious security risk, as they can compromise the accountability, traceability, and auditability of the actions and activities performed by the users or devices. Generic accounts can also enable unauthorized or malicious access, as they may have weak or default passwords, or may not have proper access control or monitoring mechanisms. User accounts, system accounts, and privileged accounts are not the types of accounts that violate identity and access management best practices, as they are accounts that have a specific or unique identity associated with them, and can be subject to proper authentication, authorization, and auditing measures.

NEW QUESTION: 652

下列哪一項是使用資料加密標準 (DES) 時初始化向量的特徵？

A. 發送者和接收者都必須知道。

B. 可以以隨機數的形式明文傳送。

C. 必須保留到最後一個區塊傳輸完畢。

D. 可用來加密和解密資訊。

Answer: (SHOW ANSWER)

According to the CISSP All-in-One Exam Guide, a characteristic of the initialization vector when using Data Encryption Standard (DES) is that it can be transmitted in the clear as a random number. An initialization vector (IV) is a value or a parameter that is used to initialize or modify the encryption or decryption process, such as the cipher block chaining (CBC) mode of operation.

An IV is used to provide an additional layer of security and randomness to the encryption or decryption process, as it prevents the same plaintext from producing the same ciphertext, and vice versa. An IV can be transmitted in the clear as a random number, as it does not contain any sensitive or confidential information, and as it changes with each session or transaction, making it difficult for the attackers to predict or manipulate the encrypted or decrypted data patterns. An IV must be known to both sender and receiver is not a characteristic of the initialization vector when using Data Encryption Standard (DES), as it is a requirement or a condition for the initialization vector when using any symmetric encryption algorithm, not a specific characteristic for DES. A symmetric encryption algorithm is an encryption algorithm that uses the same key for both encryption and decryption, such as DES, Triple DES, or Advanced Encryption Standard (AES). A symmetric encryption algorithm requires that the IV must be known to both sender and receiver, as it is needed for both encryption and decryption, and as it is used to synchronize the encryption or decryption process between the sender and the receiver. An

IV must be retained until the last block is transmitted is not a characteristic of the initialization vector when using Data Encryption Standard (DES), as it is a requirement or a condition for the initialization vector when using any block cipher algorithm, not a specific characteristic for DES. A block cipher algorithm is an encryption algorithm that divides the plaintext or the ciphertext into fixed-length blocks, and encrypts or decrypts each block separately, such as DES, Triple DES, or AES. A block cipher algorithm requires that the IV must be retained until the last block is transmitted, as it is used to link or chain the blocks together, and as it is needed for the encryption or decryption of the last block. An IV can be used to encrypt and decrypt information is not a characteristic of the initialization vector when using Data Encryption Standard (DES), as it is a function or a purpose of the initialization vector when using any encryption algorithm, not a specific characteristic for DES. An encryption algorithm is a mathematical function or procedure that transforms the plaintext or the original data into the ciphertext or the encrypted data, and vice versa, using a key or a parameter, such as DES, Triple DES, AES, or Rivest-Shamir-Adleman (RSA). An encryption algorithm uses the IV to encrypt and decrypt information, as it is a value or a parameter that is used to initialize or modify the encryption or decryption process, and as it provides an additional layer of security and randomness to the encryption or decryption process.

NEW QUESTION: 653
系統開發生命週期（SDLC）流程的安全認證任務在哪個階段結束時完成？
A. 系統取得與開發
B. 系統操作與維護
C. 系統□動
D. 系統實現
Answer: D (LEAVE A REPLY)
In the System Development Life Cycle (SDLC), security accreditation typically occurs at the end of the System Implementation phase. This phase involves the final steps of building, configuring, and deploying the system, and it is where the system undergoes rigorous testing, validation, and security reviews. The security accreditation process ensures that the system meets all security requirements and that risks are properly mitigated before the system goes live.

NEW QUESTION: 654
強制存取控制（MAC）有什麼用？
A. 允許標記敏感使用者帳□以進行存取控制
B. 允許根據敏感度強制使用使用者身分和密碼
C. 允許系統管理員對物件進行強制存取控制
D. 允許基於標籤表示的敏感度的物件安全
Answer: (SHOW ANSWER)
Mandatory access control (MAC) is a type of access control model that enforces security policies based on the classification of the subjects (users or processes) and the objects (resources or data) in a system. MAC allows for object security based on sensitivity represented by a label, which is a tag or a mark that indicates the level of confidentiality or clearance required to access the object. The label is

assigned by the system administrator or the data owner and cannot be changed by the subject. The system compares the label of the subject and the object to determine whether to grant or deny access. MAC is commonly used in military or government systems that handle classified or sensitive information.

NEW QUESTION: 655
在與其他系統建立聯合單一登入 (SSO) 解決方案時，下列何者是組織最關心的問題？
A. 向身分提供者發送斷言
B. 從合作夥伴網域請求身分斷言
C. 定義恆等映射方案
D. 資源提供者口詢身分提供者
Answer: C (LEAVE A REPLY)
Defining the identity mapping scheme presents the primary concern to an organization when setting up a federated single sign-on (SSO) solution with another. A federated SSO solution is a system that allows users to authenticate once and access multiple resources across different domains or organizations. An identity mapping scheme is a method of translating the user identities and attributes between different identity providers and resource providers. Defining the identity mapping scheme is a critical step in setting up a federated SSO solution, because it determines how the user information is exchanged and verified across the federation. Sending assertions to an identity provider, requesting identity assertions from the partner's domain, and having the resource provider query the identity provider are not the primary concerns to an organization when setting up a federated SSO solution with another, although they are part of the federated SSO process. An assertion is a statement or claim about a user's identity or attributes that is digitally signed by an identity provider. A resource provider is a system that provides access to a resource or service based on the user's identity or attributes. A resource provider may request or receive assertions from an identity provider or another resource provider to verify the user's identity or attributes.

NEW QUESTION: 656
下列哪一項是應對暴力破解登入攻擊的最佳對策？
A. 更改所有規範密碼
B. 減少同時使用者會話數
C. 僅限當面交付初始密碼
D. 在系統存取嘗試失敗後引入延遲
Answer: D (LEAVE A REPLY)
The best countermeasure to brute force login attacks is to introduce a delay after failed system access attempts. A brute force login attack is a type of attack that tries to guess the username and password of a system or account by using a large number of possible combinations, usually with the help of automated tools or scripts. A delay after failed system access attempts is a security mechanism that imposes a waiting time or a penalty before allowing another login attempt, after a certain number of unsuccessful attempts. This can slow down or discourage the brute force login attack, as it increases the time and effort required to find the correct credentials.

Changing all canonical passwords, decreasing the number of concurrent user sessions, and restricting initial password delivery only in person are not the best countermeasures to brute force login attacks, as they do not directly address the frequency or speed of the login attempts or the use of automated tools or scripts.

NEW QUESTION: 657
遠端桌面協定 (RDP) 遭到破壞的最常見原因是什麼？
A. 連接埠掃描
B. 暴力攻擊
C. 遠端利用
D. 社會工程
Answer: B (LEAVE A REPLY)
The most common cause of Remote Desktop Protocol (RDP) compromise is brute force attack.
RDP is a protocol that allows a user to remotely access and control another computer or device, over a network or the internet, using a graphical user interface. RDP can provide convenience and efficiency for the remote administration, support, or collaboration, but it can also pose a security risk, as it can expose the remote computer or device to potential attacks, such as port scan, remote exploit, social engineering, or brute force attack. Brute force attack is a type of attack that involves trying multiple combinations of usernames and passwords, until finding the correct or valid one, to gain unauthorized access to a system or a service, such as RDP. Brute force attack is the most common cause of RDP compromise, as it can exploit the weak or default credentials, or the lack of multifactor authentication, of the RDP service.

NEW QUESTION: 658
下列哪種類型的防火牆在轉送流量之前僅檢口封包之間的 握手」？
A. 代理防火牆
B. 基於主機的防火牆
C. 電路級防火牆
D. 網路位址轉換 (NAT) 防火牆
Answer: C (LEAVE A REPLY)
Circuit-level firewalls are a type of firewall that only examines the "handshaking" between packets before forwarding traffic. Circuit-level firewalls operate at the transport layer of the OSI model, and they establish a virtual circuit or session between the source and the destination hosts.
Circuit-level firewalls do not inspect the content or the header of the packets, but they only verify that the packets belong to a valid and established session. Circuit-level firewalls are faster and less resource- intensive than other types of firewalls, but they provide less security and visibility.

NEW QUESTION: 659
網路掃描發現 50% 的系統存在一個或多個嚴重漏洞。下列哪一項是最佳因應措施？
A. 評估脆弱性風險和專案有效性。

B. 評估漏洞風險和業務影響。
C. 斷開所有有嚴重漏洞的系統。
D. 斷開漏洞最多的系統。
Answer: B (LEAVE A REPLY)
The best action after finding 50% of the systems with one or more critical vulnerabilities is to assess the vulnerability risk and business impact. This means to evaluate the likelihood and severity of the vulnerabilities being exploited, as well as the potential consequences and costs for the business operations and objectives. This assessment can help prioritize the remediation efforts, allocate the resources, and justify the investments.

NEW QUESTION: 660
哪種類型的測試能□在模擬真實災難場景的情況下評估災難復原 (DR) 計劃，同時最大限度地減少對業務營運的影響？
A. 平行
B. 攻略
C. 模擬
D. 桌面
Answer: (SHOW ANSWER)
The type of test that assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations is simulation. Simulation is a type of test or a evaluation technique or method that assesses or analyzes the Disaster Recovery (DR) plan or the document that defines or specifies the procedures or the actions that are performed or executed by the organization, such as the business, the enterprise, or the institution, to recover or to restore the critical or the essential functions or operations of the organization, such as the services, the products, or the processes, after or during the occurrence or the happening of the disaster or the event that causes or results in the disruption, the interruption, or the damage of the functions or operations of the organization, such as the fire, the flood, or the cyberattack, by using or applying the realistic or the practical disaster scenarios or situations that mimic or imitate the occurrence or the happening of the disaster or the event that causes or results in the disruption, the interruption, or the damage of the functions or operations of the organization, such as the fire, the flood, or the cyberattack, but without affecting or impacting the actual or the real functions or operations of the organization, such as the services, the products, or the processes. Simulation is the type of test that assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations, as it can provide or offer the benefits, the advantages, or the value of the test or the evaluation technique or method, such as the verification, the validation, or the identification of the effectiveness, the efficiency, or the issues of the Disaster Recovery (DR) plan, and the improvement, the enhancement, or the update of the Disaster Recovery (DR) plan, by using or applying the realistic or the practical disaster scenarios or situations that mimic or imitate the occurrence or the happening of the disaster or the event that causes or results in the disruption, the interruption, or the damage of the functions or operations of the organization, such as the fire, the flood, or the cyberattack, and as it can also provide or offer the minimal or the low impact or effect to the actual or the real functions or

operations of the organization, such as the services, the products, or the processes, by using or applying the simulated or the artificial environment or setting that does not interfere or disturb the actual or the real environment or setting of the organization, such as the network, the system, or the service.

NEW QUESTION: 661
下列哪一項是跨站請求偽造 (CSRF) 的最佳定義？
A. 強制最終使用者在其目前經過驗證的 Web 應用程式上執行不必要的操作的攻擊
B. 將□本注入網頁以執行特權指令的攻擊
C. 跨安全區域發出非法請求，從而將自身偽造到系統的安全資料庫中的攻擊
D. 跨系統偽造虛假結構□詢語言 (SQL) 指令的攻擊
Answer: A (LEAVE A REPLY)
An attack which forces an end user to execute unwanted actions on a web application in which they are currently authenticated is the best definition of Cross-Site Request Forgery (CSRF).
CSRF is a type of web-based attack that exploits the trust relationship between a web browser and a web server. CSRF occurs when an attacker tricks or coerces an end user to visit a malicious website or click on a malicious link, which then sends a forged request to a web application that the end user is already logged in to. The web application, assuming that the request is legitimate and authorized, executes the request and performs the action that the attacker intended, such as transferring funds, changing passwords, or deleting data. The end user may not be aware of the CSRF attack, as it happens in the background and does not require the user's input or consent. CSRF can compromise the security and privacy of the end user and the web application, and cause financial or reputational damage to both parties.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 662
在評估網路漏洞時，探索暗網如何為滲透測試增加價□？
A. 可以隱藏用於測試的實際來源和工具。
B. 可以找到相關違規和駭客攻擊的資訊。
C. 可以在不影響測試環境的情況下測試漏洞。
D. 可以在隱藏的供應商補丁上找到資訊。
Answer: B (LEAVE A REPLY)
The dark web is often a source of illicit information, including data dumps, hacking tools, exploit kits, and discussions about known vulnerabilities, breaches, and cyberattacks. By navigating the dark web, penetration testers can gain insights into:

Exploits that attackers are using against systems, which may help in identifying vulnerabilities within the target environment.
Credential dumps and other sensitive data that may indicate a breach in the target organization or its related entities.
Discussion threads where attackers or malicious actors share techniques or vulnerabilities they are exploiting, which could be relevant to the system being tested.

NEW QUESTION: 663
以下哪□最能描述“提示注入”作□基于大型□言模型 (LLM) 构建的□用程序的安全□□？
A. 攻□者通□物理方式□坏人工智能硬件的漏洞
B. 攻□者通□构造□意□入，操□LLM(□□□□管理器)使其忽略□期指令或□生意外的、可能有害的□出，□是一种技□。
C. 一种更高效地□□LLM的方法
D. □影响□像生成模型的漏洞
Answer: B (LEAVE A REPLY)
Prompt injection is an attack technique in which a malicious actor crafts specially designed input intended to manipulate a large language model into disregarding its original system instructions or safety constraints, potentially causing it to leak sensitive information, produce harmful content, or perform unintended actions-an emerging concern as organizations increasingly integrate LLMs into applications and workflows.

NEW QUESTION: 664
下列哪一項是安全事件的直接金錢成本？
A. 士氣
B. 聲譽
C. 設備
D. 訊息
Answer: C (LEAVE A REPLY)
A direct monetary cost of a security incident refers to the immediate financial impact incurred by the organization due to the event. This can include costs for:
Repairing or replacing damaged equipment: Security incidents, such as cyberattacks or physical breaches, may damage or compromise hardware, requiring immediate replacement or repair, which comes with a direct cost.
Cost of securing or restoring affected systems: This includes expenses related to repairing or reinstalling compromised systems, software, or networks.

NEW QUESTION: 665
一名新進員工正式向組織安全團隊通報可疑行為。報導稱，與該組織無關的人正在詢問該成員的工作地點、工作期限和建築門禁管制情況。員工的檢舉最有可能是下列哪一項的結果？
A. 規避風險

B. 安全工程
C. 安全意識
D. 網路釣魚
Answer: C (LEAVE A REPLY)
Security awareness is the knowledge and understanding of security threats, risks, and best practices that enable users to protect themselves and the organization from cyberattacks.
Security awareness training is a program that educates users on how to recognize and respond to various types of security incidents, such as phishing, social engineering, malware, ransomware, etc.
The employee's reporting of the suspicious behavior is most likely the result of security awareness training, as it shows that the employee was able to identify a potential social engineering attempt and report it to the security team. Risk avoidance is a strategy that involves avoiding or eliminating activities or assets that pose a high level of risk to the organization. Risk avoidance does not explain the employee's reporting of the suspicious behavior, as it is not related to the incident. Security engineering is the application of engineering principles and practices to design and implement secure systems and processes. Security engineering does not explain the employee's reporting of the suspicious behavior, as it is not related to the incident.
Phishing is a type of social engineering attack that uses fraudulent emails or websites to trick users into revealing sensitive information or installing malware. Phishing is not the result of the employee's reporting, but rather the possible motive of the suspicious behavior.

NEW QUESTION: 666
什麼時候安全要求的實施成本最低？
A. 由外部顧問決定時
B. 在應用程式推出階段
C. 在專案週期的每個階段
D. 口建到應用程式設計時
Answer: D (LEAVE A REPLY)
The least expensive time to implement security requirements is when they are built into the application design. Here's why:
Building security into the application design ensures that security measures are considered from the very beginning of the development process. When security is incorporated during the design phase, it becomes an integral part of the architecture, rather than an afterthought. This approach is often referred to as "security by design" and is typically the most cost-effective because it avoids the need for expensive rework or retrofitting later on.
Designing security into the system early allows developers to address potential vulnerabilities in the initial design and coding phases, rather than patching security issues after the application has been built or rolled out. Fixing security problems after deployment can be very costly, as it may involve reworking large portions of the application, causing delays, and potentially disrupting business operations.

NEW QUESTION: 667

下列何者最能確保目標接收者的交易完整性？
A. 公鑰基礎設施 (PKI)
B. 區塊鏈技術
C. 預先共用金鑰 (PSK)
D. 信任網
Answer: A (LEAVE A REPLY)
The best option that ensures the integrity of transactions to intended recipients is public key infrastructure (PKI). PKI is a system that provides the services and the mechanisms for creating, managing, distributing, using, storing, and revoking the digital certificates and the public keys that are used for securing the communication and the transactions between the systems or the entities. PKI ensures the integrity of transactions to intended recipients, because it can:
Verify and authenticate the identity and the validity of the systems or the entities that are involved in the transactions, by using the digital certificates and the public keys, and prevent any impersonation, spoofing, or repudiation of the transactions.
Encrypt and decrypt the data or the information that are exchanged in the transactions, by using the public keys and the private keys, and prevent any interception, modification, or eavesdropping of the transactions.
Sign and verify the data or the information that are exchanged in the transactions, by using the digital signatures and the public keys, and ensure that the transactions are not altered, corrupted, or tampered with.

NEW QUESTION: 668
下列哪一項是使用正式安全測試報告格式和結構的主要優點？
A. 高階主管受眾將了解測試結果以及採取糾正措施的最合適的後續步驟
B. 技術團隊將了解測試目標、所應用的測試策略以及與每個漏洞相關的業務風險
C. 管理團隊將了解測試目標和組織的聲譽風險
D. 技術和管理團隊將更了解測試目標、每個測試階段的結果以及潛在的影響級別
Answer: D (LEAVE A REPLY)
A formalized security testing report provides a structured approach to communicating the findings of security tests to both technical and management teams. By using a standardized format, the report helps ensure that:
Testing objectives are clearly defined, so all stakeholders understand the purpose and scope of the testing.
The results of each test phase are presented in a consistent and easily understandable manner.
Impact levels (such as severity of vulnerabilities or risks) are well-defined, helping stakeholders evaluate the importance of the issues found and prioritize remediation efforts.
This helps both technical teams (who need to address the findings) and management teams (who need to make informed decisions on resource allocation, corrective actions, etc.) better understand the outcomes and implications of the security testing.

NEW QUESTION: 669

下列哪一項最適合收集零時差攻擊的證據？
A. 防火牆
B. 蜜罐
C. 反垃圾郵件
D. 防毒軟體
Answer: B (LEAVE A REPLY)
A honeypot is a decoy system that is designed to attract and trap attackers. A honeypot can be used to collect evidence of a zero-day attack, which is an attack that exploits a previously unknown vulnerability. A honeypot can capture the attacker's actions, tools, and techniques, and provide valuable information for analysis and mitigation. A honeypot can also divert the attacker's attention from the real targets and waste their time and resources. A firewall, an antispam, and an antivirus are not effective in detecting or preventing zero-day attacks, as they rely on known signatures or rules that may not match the new attack.

NEW QUESTION: 670
下列哪一項對組織的安全態勢影響最大？
A. 國際和特定國家的合規要求
B. 員工和承包商違反安全規定的行為
C. 由於安全支援成本不斷增加而導致的資源限制
D. 與員工存取權限流程相關的稽核結果
Answer: A (LEAVE A REPLY)
The factor that has the greatest impact on an organization's security posture is the international and country-specific compliance requirements. Compliance requirements are the rules or the regulations that an organization must follow or adhere to, in order to meet the standards or the expectations of the authorities or the stakeholders, such as the governments, the customers, or the auditors. Compliance requirements can vary depending on the location, the industry, or the type of the organization, and they can affect the security policies, the controls, or the practices of the organization. Compliance requirements can have a significant impact on the organization's security posture, as they can influence the security objectives, the risks, or the resources of the organization, and they can also impose penalties or sanctions for non-compliance or violations.

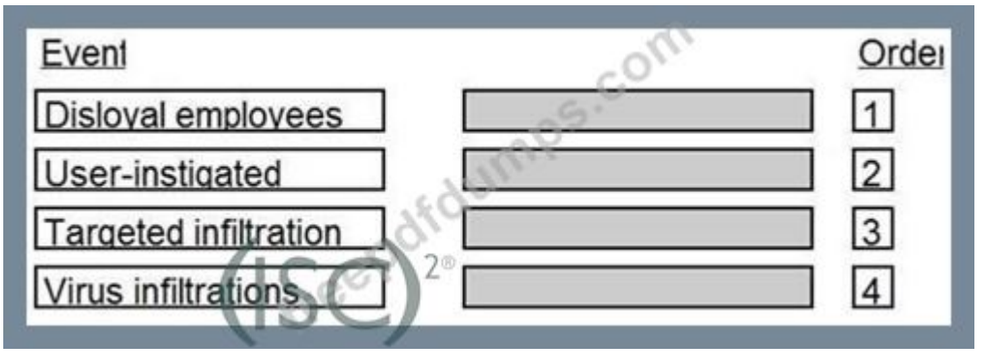
NEW QUESTION: 671
請參考以下資訊回答問題。
在對一起安全事件進行調口的過程中，確定有未經授權的個人存取了託管包含財務資訊的資料庫的系統。如果入侵導致系統進程掛起，下列哪些方面會受到影響？
A. 系統完整性
B. 系統可用性
C. 系統保密性
D. 系統可審計性
Answer: B (LEAVE A REPLY)
If the intrusion causes the system processes to hang, the system availability has been affected.

The system availability is the property or the characteristic of the system that ensures that the system is accessible and functional when needed by the authorized users or entities, and that the system is protected from the unauthorized or the malicious denial or disruption of service. The system availability can be affected when the system processes hang, as it can prevent or delay the system from responding to the requests or performing the tasks, and it can cause the system to crash or freeze. The system availability can also be affected by other factors, such as the network congestion, the hardware failure, the power outage, or the malicious attacks, such as the distributed denial-of- service (DDoS) attack. System integrity, system confidentiality, and system auditability are not the properties or the characteristics of the system that have been affected, if the intrusion causes the system processes to hang, as they are related to the accuracy, the secrecy, or the accountability of the system, not the accessibility or the functionality of the system.

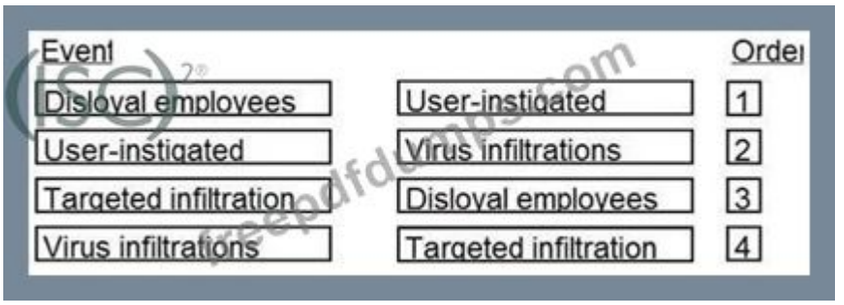
NEW QUESTION: 672
下列哪一項是使用主動發現工具執行掃描的主要目標？
A. 發現病毒和惡意軟體活動
B. 發現安全性配置管理 (CM) 的更改
C. 漏洞管理與修復
D. 資口識別 (ID) 和庫存管理
Answer: (SHOW ANSWER)

NEW QUESTION: 673
在軟體開發中，下列哪一個實體通常會對程式碼進行簽署以保護程式碼完整性？
A. 開發程式碼的組織
B. 品質控制組
C. 資料擁有者
D. 開發者
Answer: D (LEAVE A REPLY)
Code signing is the process of applying a digital signature to a piece of code to verify its authenticity and integrity. Code signing helps protect the code from unauthorized modification, tampering, or corruption. Code signing also helps users and systems to identify the source and trustworthiness of the code. In software development, the entity that normally signs the code is the developer who created or modified the code. The developer uses a private key to sign the code and a public key certificate to associate the signature with the developer's identity. The developer's signature can then be verified by anyone who has the corresponding public key or a trusted certificate authority (CA).

NEW QUESTION: 674
拖放題
使用者意識培訓依影響程度由高到低依序降低下列事件的發生率？



Answer:



NEW QUESTION: 675
以下哪□最能描述“全□加密(FDE)”的目的？
A. □加密用□□□的特定文件或文件□
B. □存□□□的全部内容□行加密，即使物理□□□失或被盗，也能保□静□数据
C. □在数据通□网□□□□□行加密
D. □□磁□上的数据以□省存□空□
Answer: B (LEAVE A REPLY)
Full Disk Encryption encrypts the entire storage volume, including the operating system, applications, and all files, ensuring that data remains protected and unreadable without the appropriate decryption key or credentials if the physical device is lost, stolen, or improperly disposed of.

NEW QUESTION: 676
A 公司正在評估新軟體以取代□部開發的應用程式。在收購過程中。A 公司指定了安全退役以及功能要求。B 公司回應了收購請求，推出了其旗艦□品，該□品運行在A 公司從未使用或評估過的作業系統(OS) 上。此旗艦□品滿足 A 公司定義的所有安全和功能要求。
根據B公司的答复，A公司應該採取什麼措施？
A. 繼續收購流程，購買旗艦軟體
B. 對作業系統進行安全審□
C. 執行功能測試
D. 進行合約談判，確保建立服務等級協定(SLA) 以包含安全補丁
Answer: (SHOW ANSWER)
Company A should conduct a security review of the OS that Company B's flagship product runs on, since it is unfamiliar to them and may introduce new risks or vulnerabilities. The security review should evaluate the OS's security features, patches, updates, configuration, and compatibility with Company A's environment. Moving ahead with the acquisition process without reviewing the OS, performing

functionality testing, or entering into contract negotiations are premature steps that may compromise Company A's security posture.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 677
下列哪一項是整合電子郵件加密系統的推薦替代方案？
A. 簽署包含敏感資料的電子郵件
B. 敏感資料請透過單獨的電子郵件發送。
C. 對附件中的敏感資料進行單獨加密
D. 將要傳送的敏感資訊儲存在加密磁碟機中
Answer: C (LEAVE A REPLY)
While integrated email encryption systems automatically encrypt the content of emails, an alternative approach to ensure the security of sensitive data in emails is to encrypt sensitive data separately in attachments. Here's why this is a good alternative:
Encryption of attachments ensures that sensitive data is protected even if the email itself is not encrypted. By encrypting the file separately, you can guarantee the confidentiality of the data, regardless of the email encryption system in use.
This method also allows the sender to control encryption keys independently of email services and recipients, as the attachment's encryption can be managed separately from the email system.

NEW QUESTION: 678
下列哪一項是使用靜態身份驗證的遠端存取協定？
A. 點對點隧道協定 (PPTP)
B. 路由資訊協定 (RIP)
C. 密碼驗證協定 (PAP)
D. 質詢握手驗證協定 (CHAP)
Answer: C (LEAVE A REPLY)
Password Authentication Protocol (PAP) is a remote access protocol that uses a static authentication method, which means that the username and password are sent in clear text over the network. PAP is considered insecure and vulnerable to eavesdropping and replay attacks, as anyone who can capture the network traffic can obtain the credentials. PAP is supported by Point-to-Point Protocol (PPP), which is a common protocol for establishing remote connections over dial-up, broadband, or wireless networks. PAP is usually used as a fallback option when more secure protocols, such as Challenge

Handshake Authentication Protocol (CHAP) or Extensible Authentication Protocol (EAP), are not available or compatible.

NEW QUESTION: 679
減少網路遭受基於 Internet 控制訊息協定 (ICMP) 的攻擊的第一步是什麼？
A. 在組織的網路邊界實施出口過濾。
B. 實施網路存取控制清單 (ACL)。
C. 實作 Web 應用程式防火牆 (WAF)。
D. 實施入侵防禦系統 (IPS)。
Answer: A (LEAVE A REPLY)
Internet Control Message Protocol (ICMP) is a protocol that is used to send and receive diagnostic and error messages between network devices, such as ping and traceroute. ICMP can also be used to launch various types of attacks, such as denial-of-service, reconnaissance, spoofing, redirection, and amplification. The first step in reducing the exposure of a network to ICMP based attacks is to implement egress filtering at the organization's network boundary, which is the point where the internal network connects to the external network, such as the internet. Egress filtering is the process of inspecting and filtering the outgoing network traffic, based on predefined rules or policies. Egress filtering can prevent or limit the ICMP traffic that originates from the internal network, which can reduce the chances of triggering or participating in ICMP attacks.

NEW QUESTION: 680
什麼原則要求明文的更改會影響密文的許多部分？
A. 擴散
B. 封裝
C. 混淆
D. 排列
Answer: A (LEAVE A REPLY)
Diffusion is the principle that requires that changes to the plaintext affect many parts of the ciphertext. Diffusion is a property of a good encryption algorithm that aims to spread the influence of each plaintext bit over many ciphertext bits, so that a small change in the plaintext results in a large change in the ciphertext. Diffusion can increase the security of the encryption by making it harder for an attacker to analyze the statistical patterns or correlations between the plaintext and the ciphertext. Encapsulation, obfuscation, and permutation are not principles that require that changes to the plaintext affect many parts of the ciphertext, as they are related to different aspects of encryption or security.

NEW QUESTION: 681
首席資訊安全長 (CISO) 關心業務應用程式的可用性。該組織最近遭受勒索軟體攻擊，導致所有主要業務流程需要紙本運行的應用程式和服務在 10 個工作天內無法使用。現在有積極的計劃來增強恢復時間目標（RTO）並滿足更頻繁的資料擷取。為了完全滿足新的業務需求，應實施下列哪些解決方案？
A. 虛擬化

B. 防毒軟體
C. 進程隔離
D. 基於主機的入侵防禦系統 (HIPS)
Answer: A (LEAVE A REPLY)
Virtualization is a solution that can help to enhance the recovery time objective (RTO) and cater for more frequent data captures, as required by the new business requirements. Virtualization is a technique that creates a virtual version of a resource, such as a server, a storage, a network, or an application, that can run on a physical platform. Virtualization can improve the availability, scalability, and performance of the resources, as well as reduce the cost, complexity, and risk of the resources. Virtualization can help to achieve a shorter RTO, which is the maximum acceptable time to restore the normal operations and services after a disruption or disaster.
Virtualization can enable faster recovery of the resources, by using techniques such as snapshots, backups, replication, or failover. Virtualization can also help to cater for more frequent data captures, which can reduce the data loss and improve the data integrity. Virtualization can enable more frequent data captures, by using techniques such as incremental backups, differential backups, or continuous data protection. Antivirus, process isolation, and host-based intrusion prevention system (HIPS) are not solutions that can help to enhance the RTO and cater for more frequent data captures, as required by the new business requirements. Antivirus is a software tool that detects and removes malicious software, such as viruses, worms, trojans, or ransomware, from a system or a network. Antivirus can help to protect the confidentiality, integrity, and availability of the data and the system, but it does not directly affect the RTO or the data capture frequency. Process isolation is a security technique that separates the processes running on a system or a network, so that they do not interfere with each other or access each other's resources. Process isolation can help to prevent the propagation, escalation, or exploitation of the processes, but it does not directly affect the RTO or the data capture frequency. Host-based intrusion prevention system (HIPS) is a security tool that monitors and blocks malicious or anomalous activities on a host, such as a server, workstation, or device. HIPS can help to protect the host from attacks, such as malware, exploits, or unauthorized changes, but it does not directly affect the RTO or the data capture frequency.

NEW QUESTION: 682
以下哪□最能描述“□□□□性□划□□”的最佳□践？
A. 制定一次□□□□性□划，然后就再也不修改了
B. 定期□□、□□和更新□□□□性□划 (BCP)，以反映□□□化、从演□或□□事件中吸取的□□教□以及不断□展的□□流程或技□。
C. □在□生重大灾害后才□□□□□□性□划
D. 将所有□□□□性□划 (BCP) □□□□完全委托□一个人，且没有□用人□。
Answer: B (LEAVE A REPLY)
Effective BCP maintenance requires regularly reviewing, testing (through tabletop exercises, walkthroughs, or full-scale simulations), and updating the plan to reflect organizational changes (such as new systems, personnel, or facilities), lessons learned from exercises or actual incidents, and

evolving business processes, ensuring the plan remains accurate and effective over time rather than becoming outdated.

NEW QUESTION: 683
下列哪一項可以保護金融服務組織所使用的個人識別資訊 (PII)？
A. 美國國家標準與技術研究院 (NIST) SP 800-53
B. 格拉姆里奇比利雷法案 (GLBA)
C. 支付卡口業資料安全標準 (PCI-DSS)
D. 健康保險流通與責任法案 (HIPAA)
Answer: B (LEAVE A REPLY)
The law that protects personally identifiable information (PII) used by financial services organizations is the Gramm-Leach-Bliley Act (GLBA). GLBA is a federal law that was enacted in
1999 to regulate the privacy and security of the financial information of the customers of financial institutions, such as banks, credit unions, insurance companies, or securities firms. GLBA requires financial institutions to provide their customers with a notice of their privacy policies and practices, and to obtain their consent before sharing their nonpublic personal information with third parties. GLBA also requires financial institutions to implement safeguards to protect the security, confidentiality, and integrity of the customer information, and to report any breaches or unauthorized access to the customers and the regulators. National Institute of Standards and Technology (NIST) SP 800-53 is a publication that provides a set of security and privacy controls for federal information systems and organizations, but it is not a law that protects PII used by financial services organizations. Payment Card Industry Data Security Standard (PCI-DSS) is a standard that provides a set of security requirements for organizations that store, process, or transmit cardholder data, such as credit card or debit card information, but it is not a law that protects PII used by financial services organizations. Health Insurance Portability and Accountability Act (HIPAA) is a law that protects the privacy and security of the health information of the patients of health care providers, health plans, or health care clearinghouses, but it is not a law that protects PII used by financial services organizations.

NEW QUESTION: 684
下列哪一項決定了根據基礎設施層的狀態如何進行交通流向？
A. 交通飛機
B. 應用平面
C. 資料平面
D. 控制平面
Answer: (SHOW ANSWER)
The control plane is the part of a network that determines how traffic should flow based on the status of the infrastructure layer. The control plane is responsible for the configuration and management of the network devices, such as routers, switches, or firewalls, and the routing protocols, such as OSPF, BGP, or RIP, that control the path selection and forwarding of the network traffic. The control plane communicates with the data plane and the management plane to ensure the optimal and secure operation of the network. The data plane is the part of a network that carries the user or application

data from the source to the destination. The data plane is responsible for the processing and forwarding of the network packets, such as IP, TCP, or UDP, that encapsulate the data. The data plane communicates with the control plane to receive the routing and forwarding instructions. The management plane is the part of a network that monitors and controls the network devices and their performance. The management plane is responsible for the administration and maintenance of the network devices, such as configuration, backup, update, or troubleshooting, and the network services, such as SNMP, SSH, or Telnet, that enable the remote access and management of the network devices. The management plane communicates with the control plane and the data plane to collect and analyze the network information and statistics. The traffic plane is not a part of a network, but rather a term that refers to the network traffic itself, or the data that flows through the network.

NEW QUESTION: 685
以下哪□最能描述使用用□和□体行□分析 (UEBA) □行“出口异常□□”的目的？
A. □了□制□行密□复□度要求
B. 建立正常用□和系□行□的基□，并□□异常情况，例如异常数据□□量或□□模式，□些都可能表明系□遭到入侵或存在内部威□。
C. □服□器机房出入口□行物理安全防□
D. 管理□件□可合□性
Answer: (SHOW ANSWER)
UEBA solutions establish baselines of normal behavior for users and entities (such as typical data access volumes, login times, and locations) and use analytics to detect significant deviations from these baselines-such as an unusual spike in outbound data transfer-that may indicate a compromised account, insider threat, or other anomalous activity warranting investigation.

NEW QUESTION: 686
購買新軟體時必須在哪些過程中考慮安全性？
A. 合約談判
B. 徵求建議書 (RFP)
C. 實施
D. 供應商選擇
Answer: B (LEAVE A REPLY)
Security must be considered during the acquisition of new software in the request for proposal (RFP) process, which is the process of soliciting bids from potential vendors and evaluating their proposals based on predefined criteria. The RFP should include the security requirements and specifications for the software, such as functionality, performance, compatibility, compliance, and testing. The RFP should also include the security evaluation criteria and methods for the vendor selection, such as security certifications, audits, reviews, and demonstrations. Security should be considered in the RFP process to ensure that the software meets the security needs and expectations of the organization, and to avoid potential risks, costs, and liabilities associated with insecure software.

NEW QUESTION: 687

下列哪一項是防止惡意軟體引進生□環境的最佳方法？
A. 從有限的零售商購買軟體
B. 驗證所有更新的雜湊金鑰或憑證金鑰
C. 不允許來自 Internet 的程式、修補程式或更新
D. 在隔離環境中測試所有新軟體
Answer: D (LEAVE A REPLY)
Testing all new software in a segregated environment is the best method to prevent malware from being introduced into a production environment. Malware is any malicious software that can harm or compromise the security, availability, integrity, or confidentiality of a system or data. Malware can be introduced into a production environment through various sources, such as software downloads, updates, patches, or installations. Testing all new software in a segregated environment involves verifying and validating the functionality and security of the software before deploying it to the production environment, using a separate system or network that is isolated and protected from the production environment. Testing all new software in a segregated environment can provide several benefits, such as:
Preventing the infection or propagation of malware to the production environment Detecting and resolving any issues or risks caused by the software Ensuring the compatibility and interoperability of the software with the production environment Supporting and enabling the quality assurance and improvement of the software

NEW QUESTION: 688
以下哪□最能描述“不可□基□□施”作□一种□代部署方法？
A. 随着□□的推移，需要手□修□和更新的基□□施
B. □种方法中，服□器或□件在部署后□不□行任何修改；而是通□部署基于版本控制□像构建的全新替□□例来□行更改。
C. 无法□控或□□的基□□施
D. 一种□□用于物理本地硬件的部署模型
Answer: B (LEAVE A REPLY)
Immutable infrastructure is a deployment approach in which servers, containers, or other components are never modified after they are deployed; instead, any change (such as a patch or configuration update) is implemented by building and deploying an entirely new instance from a version-controlled image, then decommissioning the old one-reducing configuration drift and improving consistency, auditability, and rollback capability.

NEW QUESTION: 689
持續的資訊安全監控計劃可以透過以下哪一項最好地降低風險？
A. 收集安全事件並將其關聯起來以識別異常情況
B. 促進關鍵使用者帳號活動的全系統可見性
C. 涵蓋人員、流程與技術
D. 記錄計劃□和計劃外的系統更改
Answer: C (LEAVE A REPLY)

A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology. A continuous information security monitoring program is a process that involves maintaining the ongoing awareness of the security status, events, and activities of a system or network, by collecting, analyzing, and reporting the security data and information, using various methods and tools. A continuous information security monitoring program can provide several benefits, such as:
Improving the security and risk management of the system or network by identifying and addressing the security weaknesses and gaps Enhancing the security and decision making of the system or network by providing the evidence and information for the security analysis, evaluation, and reporting Increasing the security and improvement of the system or network by providing the feedback and input for the security response, remediation, and optimization Facilitating the compliance and alignment of the system or network with the internal or external requirements and standards A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology, because it can ensure that the continuous information security monitoring program is holistic and comprehensive, and that it covers all the aspects and elements of the system or network security. People, process, and technology are the three pillars of a continuous information security monitoring program, and they represent the following:
People: the human resources that are involved in the continuous information security monitoring program, such as the security analysts, the system administrators, the management, and the users. People are responsible for defining the security objectives and requirements, implementing and operating the security tools and controls, and monitoring and responding to the security events and incidents.
Process: the procedures and policies that are followed in the continuous information security monitoring program, such as the security standards and guidelines, the security roles and responsibilities, the security workflows and tasks, and the security metrics and indicators.
Process is responsible for establishing and maintaining the security governance and compliance, ensuring the security consistency and efficiency, and measuring and evaluating the security performance and effectiveness.
Technology: the tools and systems that are used in the continuous information security monitoring program, such as the security sensors and agents, the security loggers and collectors, the security analyzers and correlators, and the security dashboards and reports. Technology is responsible for supporting and enabling the security functions and capabilities, providing the security visibility and awareness, and delivering the security data and information.

NEW QUESTION: 690
與硬體加密相比，軟體加密通常
A. 較便宜但較慢。
B. 較昂貴但較快。
C. 較昂貴且慢。
D. 更便宜、更快。
Answer: (SHOW ANSWER)

Compared with hardware cryptography, software cryptography is generally less expensive and slower. Hardware cryptography is a type of cryptography that uses dedicated hardware devices, such as chips, cards, or modules, to perform the encryption and decryption operations, and to store and manage the keys. Software cryptography is a type of cryptography that uses software programs or applications, such as libraries, packages, or tools, to perform the encryption and decryption operations, and to store and manage the keys. Compared with hardware cryptography, software cryptography is generally less expensive, as it does not require any additional or specialized hardware devices or components, and it can be easily installed and updated on the existing systems or platforms. However, software cryptography is also generally slower, as it consumes more CPU and memory resources, and it depends on the performance and the capacity of the systems or platforms. Software cryptography can also be more vulnerable to various attacks or threats, such as malware, reverse engineering, or tampering, as it is exposed to the operating system and the network environment, and it does not have any physical or logical protection mechanisms.

NEW QUESTION: 691
資訊長 (CIO) 決定，作為業務現代化工作的一部分，組織將轉向雲端架構所有關鍵業務資料將在未來兩年口遷移到口部或外部雲端服務。CIO 的主要義務是與擔任哪個角色的人員合作，以確保在雲端遷移期間和之後正確保護資料？
A. 資訊擁有者
B. 總法律顧問
C. 首席資訊安全長 (CISO)
D. 首席安全長 (CSO)
Answer: (SHOW ANSWER)
The role that the CIO has a primary obligation to work with in order to ensure proper protection of data during and after the cloud migration is the Chief Information Security Officer (CISO). The CISO is the senior executive who is responsible for establishing, implementing, and maintaining the information security strategy, policies, and programs of the organization, and for ensuring the alignment and integration of the information security objectives and activities with the business goals and operations of the organization. The CISO is the role that the CIO has a primary obligation to work with in order to ensure proper protection of data during and after the cloud migration, as the CISO can provide the leadership, guidance, and expertise for the information security aspects of the cloud migration, such as the risk assessment, the security controls, the compliance requirements, the incident response, and the security monitoring of the cloud services.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest**

Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 692
某個組織正在嘗試透過其網路邊界保護即時訊息 (IM) 通訊的安全。下列哪一項是最重大的挑戰？
A. IM 用口端可以在多個供應商之間互通。
B. IM 用口端無需管理員權限即可運作。
C. IM 用口端可以使用隨機連接埠號碼。
D. IM 用口端可以作為可執行檔運行，無需安裝。
Answer: C (LEAVE A REPLY)
The most significant challenge when trying to secure instant messaging (IM) communications through the network perimeter is that IM clients can utilize random port numbers. IM is a form of real-time communication that allows users to exchange text, voice, video, or other data over the internet. IM clients are applications that enable users to connect to IM servers or networks, such as Skype, WhatsApp, or Telegram. IM clients can pose a security risk for the network perimeter, which is the boundary between the internal and external networks, where firewalls, routers, or other devices are used to filter and control the network traffic. IM clients can utilize random port numbers, which are the endpoints of communication between the source and destination devices, to bypass the network perimeter security. IM clients can dynamically change the port numbers they use, or use nonstandard or unregistered port numbers, to evade the detection or blocking by the network perimeter devices. IM clients can also use port hopping, which is the technique of switching the port numbers frequently, to avoid the network perimeter security. IM clients can also tunnel their traffic through other protocols, such as HTTP or HTTPS, which are usually allowed by the network perimeter devices, to conceal their communication.

NEW QUESTION: 693
某個組織實施了密碼複雜性和帳口鎖定策略，強制在十分鐘口嘗試五次錯誤登入。網路使用者報告帳口鎖定數量顯著增加。該公司影響下列哪一項安全原則？
A. 可用性
B. 誠信
C. 保密性
D. 身份驗證
Answer: A (LEAVE A REPLY)
The security principle that this company is affecting is availability, which is the ability of authorized users to access and use the resources and information of the system or network. By implementing a password complexity and an account lockout policy, the company is trying to enhance the security and authentication of the system or network, but it may also reduce the availability of the system or network for the legitimate users. If the users forget their passwords, or enter them incorrectly, or become victims of brute-force or denial-of-service attacks, they may be locked out of the system or network, and unable to perform their tasks or functions. Therefore, the company should balance the security and availability

of the system or network, and consider the impact of the password and account lockout policy on the users and the business.

NEW QUESTION: 694
將資口所有權分配給部門時，下列哪一項最重要？
A. 部門應向企業主報告
B. 應定期檢討資口的所有權
C. 應確保個人責任
D. 所有成員都應接受有關其職責的培訓
Answer: (SHOW ANSWER)
When assigning ownership of an asset to a department, the most important factor is to ensure individual accountability for the asset. Individual accountability means that each person who has access to or uses the asset is responsible for its protection and proper handling. Individual accountability also implies that each person who causes or contributes to a security breach or incident involving the asset can be identified and held liable. Individual accountability can be achieved by implementing security controls such as authentication, authorization, auditing, and logging.

NEW QUESTION: 695
誰負有確保安全目標與組織目標一致的主要責任？
A. 高階管理層
B. 資訊安全部門
C. 審計委員會
D. 所有用口
Answer: A (LEAVE A REPLY)
The primary responsibility for ensuring that security objectives are aligned with the organization's goals lies with senior management. Here's why:
Senior management is responsible for setting the strategic direction of the organization, and security is a critical component of the overall business strategy. They must ensure that security policies, initiatives, and goals are integrated into the organization's overall business objectives and risk management framework. This alignment helps ensure that security efforts support the organization's mission, protect its assets, and contribute to long-term success.
Senior management is also responsible for resource allocation and for ensuring that sufficient budget and support are provided for security programs. They must ensure that security is not just a technical issue but a fundamental part of the organizational culture and strategy.

NEW QUESTION: 696
當口部審口發現遠端存取的網路設計有缺陷時，虛擬私人網路(VPN) 設備在網路中的最佳放置位置是什麼？
A. 在指定的非軍事區(DMZ)口
B. 在其獨立的虛擬區域網路 (VLAN) 中
C. 網際網路服務供應商 (ISP)

D. 外部防火牆外

Answer: (SHOW ANSWER)

The best location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access is in a dedicated Demilitarized Zone (DMZ). A DMZ is a network segment that is located between the internal network and the external network, such as the internet. A DMZ is used to host the services or devices that need to be accessed by both the internal and external users, such as web servers, email servers, or VPN devices. A VPN device is a device that enables the establishment of a VPN, which is a secure and encrypted connection between two networks or endpoints over a public network, such as the internet. Placing the VPN devices in a dedicated DMZ can help to improve the security and performance of the remote access, as well as to isolate the VPN devices from the internal network and the external network. Placing the VPN devices in its own separate VLAN, at the ISP, or outside the external firewall are not the best locations, as they may expose the VPN devices to more risks, reduce the control over the VPN devices, or create a single point of failure for the remote access.

NEW QUESTION: 697

配置唯一使用者 ID 的最重要原因是什麼？

A. 支持問責制

B. 減少身份驗證錯誤

C. 防止密碼洩露

D. 支援單一登入(SSO)

Answer: A (LEAVE A REPLY)

Unique user IDs are essential for supporting accountability, which is the ability to trace actions or events to their source. Accountability is a key principle of security and helps to deter, detect, and correct unauthorized or malicious activities. Without unique user IDs, it would be difficult or impossible to identify who performed what action on a system or network. Reducing authentication errors, preventing password compromise, and supporting Single Sign On (SSO) are all possible benefits of using unique user IDs, but they are not the most important reason for configuring them.

NEW QUESTION: 698

下列哪一項是使用手動補丁安裝而不是自動補丁管理的原因？

A. 安裝補丁所需的成本將會降低。

B. 系統容易受到攻擊的時間將會減少。

C. 系統或應用程式不相容的可能性將會降低。

D. 覆蓋大範圍地理區域的能力增強。

Answer: C (LEAVE A REPLY)

Manual patch installation allows for thorough testing before deployment to ensure that the patch does not introduce new vulnerabilities or incompatibilities. Automated patch management can sometimes lead to unexpected issues if patches are not fully compatible with all systems and applications

NEW QUESTION: 699

拖放問題

將左側的以下安全工程術語拖曳至右側的最佳定義。

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

freepdfdumps.com

Answer:

Security Engineering Term		Definition
Risk	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	Security Risk Treatment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	Protection Needs Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	Threat Assessment	The method used to identify feasible security risk mitigation options and plans.

freepdfdumps.com

NEW QUESTION: 700

一位經常出差到不同國家的資訊科技(IT)員工遠端連接到組織的資源以排除故障。下列哪項解決方案最能作為滿足組織要求的安全控制機制？

A. 更新防火牆規則，使其包含員工連線位置的靜態網際網路通訊協定(IP) 位址。

B. 安裝第三方螢幕共享解決方案，該方案可透過公共網站提供遠端連線。

C. 實現動態網域名稱服務 (DDNS) 帳口，以使用DDNS 記錄口動虛擬私人網路 (VPN)。

D. 在非軍事區(DMZ)安裝堡壘主機，並允許多因素身份驗證(MFA)存取。

Answer: D (LEAVE A REPLY)

A bastion host is a hardened server that is placed in the demilitarized zone (DMZ), a network segment that is exposed to the internet and separated from the internal network by firewalls. A bastion host provides a secure and controlled access point for remote users or administrators who need to connect to the internal network or systems. A bastion host can also act as a proxy server, a VPN gateway, or a jump server, depending on the configuration and the purpose. A bastion host should be protected by multiple layers of security, such as multi-factor authentication (MFA), encryption, logging, monitoring, and patching. A bastion host is the best solution to allow an IT employee who travels frequently to various locations to troubleshoot problems remotely, as it minimizes the exposure and the risk of unauthorized access.

NEW QUESTION: 701

在計劃執行檢口行動模型的「執行」階段，執行下列哪一項操作？

A. 根據業務連續性政策和目標監控和審口績效，將結果報告給管理層進行審口，並確定和授權補救和改進措施。

B. 根據管理評審的結果採取糾正措施，維護和改進業務連續性管理(BCM) 系統。

C. 確保業務連續性政策、控制、流程和程序已實施。

D. 確保已建立與提高業務連續性相關的業務連續性政策、目標、指標、控制、流程和程序。

Answer: (SHOW ANSWER)

The Plan-Do-Check-Act (PDCA) model is a four-step iterative process for implementing, maintaining, and improving a management system, such as a Business Continuity Management (BCM) system.
The PDCA model consists of the following phases:
Plan: Establish the objectives, scope, and requirements of the BCM system, and develop the business continuity policy, strategy, plans, and procedures.
Do: Implement the business continuity policy, controls, processes, and procedures, and conduct the necessary training, awareness, and testing activities.
Check: Monitor and review the performance and effectiveness of the BCM system against the business continuity policy and objectives, and report the results and findings to the management for review.
Act: Maintain and improve the BCM system by taking corrective and preventive actions, based on the results of the management review and the feedback from the stakeholders. In the "Do" phase of the PDCA model, the main activity is to ensure the business continuity policy, controls, processes, and procedures have been implemented, as planned in the previous phase. This involves allocating the necessary resources, roles, and responsibilities, and executing the business continuity plans and procedures in accordance with the business continuity strategy.

This also involves providing the appropriate training and awareness programs to the staff and the relevant parties, and conducting the regular testing and exercising of the business continuity plans and procedures, to verify their functionality and suitability.

NEW QUESTION: 702
技術人員想要在房間中央安裝 WAP，在無線電周圍的半徑範圍口提供服務。AP 應使用下列哪一種天線類型？
A. 全向
B. 定向
C. 八木
D. 口物線
Answer: A (LEAVE A REPLY)
An omni antenna is a type of antenna that radiates radio signals in all directions equally. It is also known as an omnidirectional antenna or a dipole antenna. An omni antenna is suitable for a wireless access point (WAP) that is installed in the center of a room that provides service in a radius surrounding the radio, as it can cover a large area and reach multiple devices.

NEW QUESTION: 703
下列哪一項定義了網際網路協定安全(IPSec)的金鑰交換？
A. 安全通訊端層 (SSL) 金鑰交換
B. 網際網路金鑰交換(IKE)
C. 安全金鑰交換(SKE)
D. 網際網路控制訊息協定(ICMP)
Answer: B (LEAVE A REPLY)
Internet Key Exchange (IKE) is a protocol that defines the key exchange for Internet Protocol Security (IPSec). IPSec is a suite of protocols that provides security for IP-based communications, such as encryption, authentication, and integrity. IKE establishes a secure channel between two parties, negotiates the security parameters, and generates the cryptographic keys for IPSec.

NEW QUESTION: 704
下列哪一項有助於防止不當的會話處理？
A. 確保所有 UIWebView 呼叫在沒有正確輸入驗證的情況下不會執行。
B. 確保標記口長、複雜且偽隨機。
C. 確保停用 JavaScript 和外掛程式支援。
D. 確保憑證有效且關閉失敗。
Answer: B (LEAVE A REPLY)
The best way to prevent improper session handling is to ensure that tokens are sufficiently long, complex, and pseudo-random. Session handling is a process of managing the state and interaction of a user with a web application or service. Session handling typically involves creating, maintaining, and terminating a session, which is a temporary and unique identifier that links the user to the web

application or service. A session token is a value that is generated and assigned to the user when the user authenticates to the web application or service, and it is used to track and validate the user's requests and responses. A session token is usually stored in a cookie, a hidden field, or a URL parameter, and it is sent along with each request and response.
Improper session handling is a security risk that occurs when the session token is exposed, intercepted, guessed, or stolen by an attacker, who can then use it to impersonate or hijack the user's session, and gain unauthorized access or privileges to the web application or service. To prevent improper session handling, the session token should be sufficiently long, complex, and pseudo-random, meaning that it should have enough length and entropy to resist brute-force or dictionary attacks, and it should be generated using a secure random number generator that produces unpredictable and non-repeating values. Ensuring that all UIWebView calls do not execute without proper input validation, ensuring JavaScript and plugin support is disabled, and ensuring that certificates are valid and fail closed are not the best ways to prevent improper session handling, as they are not directly related to the session token generation or management, or they may not be applicable or feasible in all scenarios.

NEW QUESTION: 705
什麼類型的攻擊會向目標電腦發送 Internet 控制訊息協定 (ICMP) 回顯請求，其有效負載超出目標的處理能力？
A. 中間人 (MITM)
B. 拒口服務 (DoS)
C. 網域名稱伺服器 (DNS) 中毒
D. 緩衝區溢出
Answer: (SHOW ANSWER)
The type of attack described in the question is a Denial of Service (DoS) attack, specifically a Ping of Death attack. In this attack, the attacker sends ICMP echo requests (ping requests) to a target machine with a larger payload than the target can handle. This can cause the target system to crash, freeze, or become unresponsive, effectively denying service to legitimate users.
In a Ping of Death attack, the oversized packet is crafted to exploit vulnerabilities in the target system's handling of large ICMP packets. Modern systems typically handle these packets without issue, but older or improperly configured systems may not handle the oversized payload correctly, leading to crashes or other issues.

NEW QUESTION: 706
與安全審口週期相關的審計的主要目的是什麼？
A. 確保組織的控制和老虎機能如預期運作
B. 確保組織仍可公開交易
C. 確保組織的執行團隊不會被起訴
D. 確保組織符合合約要求
Answer: A (LEAVE A REPLY)

Auditing is the process of examining and evaluating the organization's security controls and policies, such as access control, encryption, backup, incident response, or disaster recovery, to determine if they are working as intended, and if they are compliant with the organization's objectives, standards, and regulations. Auditing is an essential part of the security review cycle, which is the process of continuously monitoring, assessing, and improving the organization's security posture. The primary purpose of auditing, as it relates to the security review cycle, is to ensure the organization's controls and policies are working as intended, and to identify and report any gaps, weaknesses, or violations that may affect the organization's security. Auditing does not necessarily ensure the organization can still be publicly traded, as this depends on other factors, such as the financial performance, the market demand, or the legal compliance of the organization. Auditing does not necessarily ensure the organization's executive team won't be sued, as this depends on other factors, such as the nature, severity, or responsibility of the security incidents or breaches that may occur in the organization. Auditing does not necessarily ensure the organization meets contractual requirements, as this depends on the specific terms and conditions of the contracts that the organization has with its customers, partners, or suppliers.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 707
認證認可過程的組態管理與控制任務納入系統開發生命週期（SDLC）的哪個階段？
A. 系統取得與開發
B. 系統操作與維護
C. 系統□動
D. 系統實現
Answer: A (LEAVE A REPLY)
The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the System Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:
System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and establishing the project plan and budget.

System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.
System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.
System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.
The certification and accreditation process is a process that involves assessing and verifying the security and compliance of a system, and authorizing and approving the system operation and maintenance, using various standards and frameworks, such as NIST SP 800-37 or ISO/IEC 27001. The certification and accreditation process can be divided into several tasks, each with its own objectives and activities, such as:
Security categorization: This task involves determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures.
Security planning: This task involves defining the security objectives and requirements of the system, identifying the roles and responsibilities of the security stakeholders, and developing and documenting the security plan and policy.
Security implementation: This task involves implementing and enforcing the security controls and measures for the system, according to the security plan and policy, and ensuring the security functionality and compatibility of the system.
Security assessment: This task involves evaluating and testing the security effectiveness and compliance of the system, using various techniques and tools, such as audits, reviews, scans, or penetration tests, and identifying and reporting any security weaknesses or gaps.
Security authorization: This task involves reviewing and approving the security assessment results and recommendations, and granting or denying the authorization for the system operation and maintenance, based on the risk and impact analysis and the security objectives and requirements.
Security monitoring: This task involves monitoring and updating the security status and activities of the system, using various methods and tools, such as logs, alerts, or reports, and addressing and resolving any security issues or changes.
The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the SDLC, because it can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system changes are controlled and documented.
Configuration management and control is a process that involves establishing and maintaining the baseline and the inventory of the system components and resources, such as hardware, software, data, or documentation, and tracking and recording any modifications or updates to the system

components and resources, using various techniques and tools, such as version control, change control, or configuration audits. Configuration management and control can provide several benefits, such as:
Improving the quality and security of the system design and development by identifying and addressing any errors or inconsistencies Enhancing the performance and efficiency of the system design and development by optimizing the use and allocation of the system components and resources Increasing the compliance and alignment of the system design and development with the security objectives and requirements by applying and enforcing the security controls and measures Facilitating the monitoring and improvement of the system design and development by providing the evidence and information for the security assessment and authorization

NEW QUESTION: 708
以下哪□最能描述 SOAR 平台中“出口点自□□本响□”在已确□的网□□□事件中的作用？
A. 人工□核每一份□□□告，没有任何自□化操作。
B. 在确□□□到网□□□□件后，自□□行□定□的一系列响□操作，例如隔离所有□箱中的□意□件、阻止□件人域以及禁用被盗用的□□。
C. 自□□除□□内所有□子□件，无□其内容如何。
D. 回复任何□□□件前，必□□得董事会全体成□的批准。
Answer: (SHOW ANSWER)
A SOAR automated playbook for a confirmed phishing incident can execute a predefined sequence of response actions-such as automatically removing the malicious email from all affected mailboxes, blocking the sender's domain or IP at the email gateway, and disabling any compromised accounts-significantly reducing response time compared to a fully manual process, while still allowing human analysts to review and approve higher-risk actions as needed.

NEW QUESTION: 709
請參考以下資訊回答問題。
一位新員工獲配一台擁有完整管理員權限的筆記型電腦。該員工家中沒有個人電腦，他的孩子會使用這台電腦收發電子郵件、上網和使用即時通訊工具。公司資訊科技部門發現，有人利用該員工的權限在電腦上安裝了一款點對點程式。
當電腦連接到辦公室網路時，下列哪一種解決方案最有可能偵測到點對點程式的使用？
A. 防毒軟體
B. 入侵防禦系統(IPS)
C. 反間諜軟體
D. 完整性檢□軟體
Answer: (SHOW ANSWER)
The best solution to detect the use of P2P programs when the computer was connected to the office network is an Intrusion Prevention System (IPS). An IPS is a device or a software that monitors, analyzes, and blocks the network traffic based on the predefined rules or policies, and that can prevent or stop any unauthorized or malicious access or activity on the network, such as P2P programs. An IPS

can detect the use of P2P programs by inspecting the network packets, identifying the P2P protocols or signatures, and blocking or dropping the P2P traffic. Anti-virus software, anti-spyware software, and integrity checking software are not the best solutions to detect the use of P2P programs when the computer was connected to the office network, as they are related to the protection, removal, or verification of the software or files on the computer, not the monitoring, analysis, or blocking of the network traffic.

NEW QUESTION: 710
以下哪□最能描述防火□上“出口□□”控制的用途？
A. 阻止来自不受信任的外部来源的入站流量
B. □控和限制离开网□的出站流量，以□□或防止数据泄露和未□授□的通信
C. 自□加密所有离开网□的流量
D. 跨多个服□器□行□□均衡
Answer: (SHOW ANSWER)
Egress filtering controls and monitors outbound traffic leaving a network, helping to detect or prevent data exfiltration, command-and-control communication from compromised hosts, and other unauthorized outbound connections, complementing ingress filtering, which focuses on inbound traffic.

NEW QUESTION: 711
發生違規事件後，調□人員將攻擊範圍縮小到特定網路管理員的憑證。然而，沒有證據表明駭客是如何獲得憑據的。根據上述調□，以下大部分行動可以最好地避免上述違規行為嗎？
A. 定期檢視網路存取遺失情況
B. 定期檢視網路中的活躍用□
C. 定期檢視所有特權帳□操作
D. 定期檢視組織□所有使用者的密碼強度
Answer: C (LEAVE A REPLY)
A periodic review of all privileged accounts actions could have best avoided the breach incident that involved a network administrator's credentials. A privileged account is an account that has elevated permissions or access rights to a system or resource, such as a network administrator, a database administrator, or a root user. Privileged accounts pose a high risk to the security of an organization, as they can be exploited by malicious insiders or external attackers to compromise the system or resource. A periodic review of all privileged accounts actions is a good practice to monitor and audit the activities and behaviors of the privileged users, and to detect and prevent any unauthorized or suspicious actions. A periodic review of network access logs, active users on the network, and password strength of all users across the organization are also good practices to enhance the security of an organization, but they are not as effective as a periodic review of all privileged accounts actions, as they may not capture the specific actions of the privileged users or the source of the breach.

NEW QUESTION: 712
以下哪个□□用于安全地解析域名，同□提供数据源□□和完整性保□？
A. DNS

B. DNSSEC
C. DHCP
D. LDAP
Answer: B (LEAVE A REPLY)
DNSSEC (Domain Name System Security Extensions) adds cryptographic signatures to DNS records, providing data origin authentication and integrity protection, allowing resolvers to verify that DNS responses have not been tampered with, mitigating attacks such as cache poisoning.

NEW QUESTION: 713
某個組織已確定其先前的軟體開發瀑布式方法無法跟上業務需求。為了適應口品交付所需的快速變化，該組織決定轉向敏捷軟體開發和發布週期。為了確保敏捷方法的成功，誰在為每個版本建立驗收測試或驗收標準方面最關鍵？
A. 專案經理
B. 軟體開發人員
C. 獨立測試人員
D. 商業客口
Answer: D (LEAVE A REPLY)
Business customers are the most critical in creating acceptance tests or acceptance criteria for each release in an Agile software development and release cycle. Acceptance tests or acceptance criteria are the requirements or specifications that define the expected functionality, quality, and performance of the system or the product, and that must be met or satisfied before the system or the product is delivered or deployed. Business customers are the stakeholders who have the authority, interest, and need for the system or the product, and who can provide the feedback, input, and validation for the acceptance tests or acceptance criteria. Business customers can help to ensure that the acceptance tests or acceptance criteria are aligned with the business goals, needs, and expectations, and that the system or the product delivers the value and benefits that the business customers require.

NEW QUESTION: 714
請參考以下資訊回答問題。
遭受財務衝擊的組織被迫削減預算，並減少負責基本邏輯存取安全管理職能的資訊科技IT)維運人員數量。安全流程已與常規IT運作緊密整合，並非獨立且不同的職能。
下列哪一項能口顯示在此期間IT預算的最佳分配方向？
A. 政策
B. 框架
C. 指標
D. 指南
Answer: (SHOW ANSWER)
The best indicator of where the IT budget is best allocated during this time is the metrics. The metrics are the measurements or the indicators of the performance, the effectiveness, the efficiency, or the quality of the IT processes, activities, or outcomes. The metrics can help to allocate the IT budget in a

rational, objective, and evidence-based manner, as they can show the value, the impact, or the return of the IT investments, and they can identify the gaps, the risks, or the opportunities for the IT improvement or enhancement. The metrics can also help to justify, communicate, or report the IT budget allocation to the senior management or the stakeholders, and to align the IT budget allocation with the business needs and requirements. Policies, frameworks, and guidelines are not the best indicators of where the IT budget is best allocated during this time, as they are related to the documents or the models that define, guide, or standardize the IT processes, activities, or outcomes, not the measurements or the indicators of the IT performance, effectiveness, efficiency, or quality.

NEW QUESTION: 715
下列哪一項是導致基於 Web 的應用程式發生安全事件的主要原因？
A. 系統管理與作業系統
B. 系統不相容性和修補程式管理
C. 第三方應用程式與變更控制
D. 壓力測試和應用程式介面不當
Answer: D (LEAVE A REPLY)
Improper stress testing and application interfaces primarily contribute to security incidents in web-based applications. Stress testing is a type of performance testing that evaluates how a web- based application behaves under extreme or abnormal conditions, such as high traffic, heavy load, or limited resources. Stress testing can help identify the potential bottlenecks, errors, or failures that may affect the functionality, reliability, or security of the web-based application.
Improper stress testing can result in undetected vulnerabilities or weaknesses that can be exploited by attackers. Application interfaces are the points of interaction between a web-based application and other systems, components, or users. Application interfaces can include web services, APIs, user interfaces, or network protocols. Application interfaces can introduce security risks if they are not designed, implemented, or secured properly. For example, application interfaces may expose sensitive data, allow unauthorized access, or enable injection attacks

NEW QUESTION: 716
下列哪一項是針對中間人 (MITM) 網際網路協定語音 (VoIP) 攻擊的最佳緩解做法？
A. 使用媒體閘道控制協定 (MGCP)
B. 使用傳輸層安全性 (TLS) 協定
C. 使用檔案傳輸協定 (FTP)
D. 使用安全外殼 (SSH) 協定
Answer: B (LEAVE A REPLY)
The best mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks is to use Transport Layer Security (TLS) protocol. TLS is a protocol that provides secure and encrypted communication and connection between two systems or devices over an unsecured or public network, such as the internet. TLS can mitigate MITM VoIP attacks, because it can:

Verify and authenticate the identity and the validity of the systems or devices that are involved in the VoIP communication or connection, by using the digital certificates and the public keys, and prevent any impersonation, spoofing, or repudiation of the VoIP communication or connection.
Encrypt and decrypt the data or the information that are exchanged in the VoIP communication or connection, by using the public keys and the private keys, and prevent any interception, modification, or eavesdropping of the VoIP communication or connection.
Sign and verify the data or the information that are exchanged in the VoIP communication or connection, by using the digital signatures and the public keys, and ensure that the VoIP communication or connection are not altered, corrupted, or tampered with.

NEW QUESTION: 717
一家大型律師事務所希望讓員工能□參與自備設備 (BYOD) 計畫。只有安裝有最新防毒軟體和作業系統 (OS) 修補程式的裝置才允許連接網路。哪種解決方案最能滿足安全要求？
A. 入侵偵測與防禦系統 (IDPS)
B. 網路存取控制 (NAC)
C. 下一代防火牆
D. 端點偵測與回應
Answer: B (LEAVE A REPLY)

NEW QUESTION: 718
透過仔細對齊鎖芯中的銷釘，下列哪一項定義了無需正確鑰匙即可打開機械鎖？
A. 鎖定 ping
B. 開鎖
C. 鎖碰撞
D. 鎖磚
Answer: B (LEAVE A REPLY)
The opening of a mechanical lock without the proper key by carefully aligning the pins in the lock is defined as lock picking. A mechanical lock is a device that secures an entry point, such as a door, a window, or a cabinet, by using a physical mechanism, such as a pin tumbler, a wafer, or a disc detainer. A mechanical lock requires a proper key to unlock it, which matches the configuration of the mechanism. Lock picking is a technique of manipulating the mechanism of the lock without the proper key, usually by using tools, such as picks, tension wrenches, or rakes.
Lock picking can exploit the flaws or weaknesses of the lock, such as the variations, tolerances, or defects of the pins or the cylinder. Lock picking can be used for legitimate purposes, such as locksmithing, hobby, or sport, or for illegitimate purposes, such as burglary, espionage, or sabotage.

NEW QUESTION: 719
以下哪□最能描述“基于地理位置的出口□□”作□一种安全控制措施？
A. 无□来源如何，都阻止所有入站流量
B. 限制或□控与正常□□运□不符的地理区域或国家的出站网□□接，□可能表明存在向未□授□目的地泄露数据的行□。

C. 自□将数据翻□成不同□言
D. □根据一天中的□□□□流量
Answer: B (LEAVE A REPLY)
Geolocation-based egress filtering restricts or closely monitors outbound connections to countries or regions that are not consistent with an organization's normal business operations, helping to detect or prevent data exfiltration to unauthorized destinations, particularly useful when combined with threat intelligence about regions associated with known malicious infrastructure.

NEW QUESTION: 720
滲透測試之後，組織應該先做什麼？
A. □看所有安全政策和程序。
B. 確保員工接受安全訓練。
C. 確定您是否需要進行全面的安全評估。
D. 評估測試結果中發現的問題。
Answer: (SHOW ANSWER)
After a penetration test, the first thing an organization should do is evaluate the problems identified in the test result. This evaluation helps prioritize the vulnerabilities and weaknesses uncovered during the test based on their severity and potential impact on the organization. By analyzing the results, the organization can take informed steps to address the most critical issues first, and plan remediation actions effectively.

NEW QUESTION: 721
一家零售公司計劃□動一個開發項目，該項目將首次在其程式碼中使用開源元件。開發團隊已經取得了多個開源元件，並在概念驗證(POC) 程式碼中使用了它們。團隊認為，開源軟體的使用帶來的益處遠大於其法律和營運風險。
組織接下來必須做什麼？
A. 強制要求所有開源元件必須經過資訊安全經理(ISM)的批准。
B. 掃描所有開源元件是否有安全漏洞。
C. 制定開源合規政策。
D. 要求所有開源元件都必須獲得商業支援。
Answer: C (LEAVE A REPLY)
Establishing an open-source compliance policy is the action that the organization must do next when looking to start a development project that will utilize open source components in its code for the first time. Open source components are the software components that are licensed under the open source licenses, and that allow the users to access, modify, and distribute the source code of the software components, such as the libraries, frameworks, or tools. Open source components can offer benefits such as cost savings, innovation, collaboration, or customization, but they can also pose risks such as security vulnerabilities, legal liabilities, or operational challenges. Establishing an open- source compliance policy is the action that involves defining and documenting the rules, guidelines, and procedures for the acquisition, use, and management of the open source components in the

development project, and that aligns with the legal and operational requirements and standards that apply to the open source components, such as the license terms, the attribution obligations, the security controls, or the quality assurance.
Establishing an open-source compliance policy is the action that the organization must do next when looking to start a development project that will utilize open source components in its code for the first time, because it can provide the following benefits:
It can ensure the compliance and adherence of the development team and the organization to the open source licenses and the legal and regulatory requirements and standards, and avoid or minimize the liabilities or penalties that may arise from the non-compliance or violation of the licenses or the requirements or standards.
It can protect the security and integrity of the development project and the organization, and prevent or mitigate the risks of security vulnerabilities, flaws, or defects that may affect the open source components or the software products that use the open source components.
It can improve the efficiency and quality of the development project and the organization, and enable the effective and consistent acquisition, use, and management of the open source components, and the integration and compatibility of the open source components.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 722
下列哪一個例子最能反映管理階層對保護安全資口和資源的承諾不足？
A. 安全流程與程序管理不善
B. 不成熟的安全控制與程序
C. 與監理要求的偏差
D. 安全事件與威脅的意外增加
Answer: A (LEAVE A REPLY)
The best example of weak management commitment to the protection of security assets and resources is poor governance over security processes and procedures. Governance is the set of policies, roles, responsibilities, and processes that guide, direct, and control how an organization's business divisions and IT teams cooperate to achieve business goals.
Management commitment is essential for effective governance, as it demonstrates the leadership and support for security initiatives and activities. Poor governance indicates that management does not prioritize security, allocate sufficient resources, enforce accountability, or monitor performance.

NEW QUESTION: 723
需要設定下列哪一項才能確保具有特定 MAC 位址的裝置始終從 DHCP 指派相同的 IP 位址？
A. 範圍選項
B. 預訂
C. 動態賦口
D. 排除
E. 靜態賦口
Answer: B (LEAVE A REPLY)
A reservation is a feature of DHCP that allows a device with a specific MAC address to be always assigned the same IP address from the DHCP server. A reservation is configured by mapping the MAC address of the device to the desired IP address on the DHCP server. This ensures that the device will always receive the same IP address, regardless of the lease time or the availability of other IP addresses in the DHCP pool.

NEW QUESTION: 724
在處理生物辨識身分驗證時，下列哪一項通常表示重播攻擊？
A. 錯誤接受率 (FAR) 大於十萬分之一
B. 錯誤拒口率 (FRR) 大於 100 中的 5
C. 指定的模板不充分
D. 完全匹配
Answer: D (LEAVE A REPLY)
The indicator that is generally indicative of a replay attack when dealing with biometric authentication is an exact match. A replay attack is a type of attack or a threat that aims or intends to bypass or to break the authentication or the verification mechanism or process of a system or a service, by capturing or recording the authentication or the verification data or information, such as the username, the password, or the token, and replaying or resending the authentication or the verification data or information to the system or the service, as if it was the legitimate or the authentic user or device. A replay attack can result or lead to the unauthorized or the inappropriate access or login to the system or the service, by the attacker or the malicious actor. Biometric authentication is a type of authentication or a verification mechanism or process that uses or applies the biometric features or characteristics of the user or the device, such as the fingerprint, the iris, or the voice, to identify or to authenticate the user or the device, and to grant or to deny the access or the login to the system or the service. Biometric authentication can provide a high level of security or protection for the system or the service, as it can prevent or reduce the risk of impersonation, duplication, or sharing of the biometric features or characteristics of the user or the device. However, biometric authentication can also be vulnerable or susceptible to the replay attack, as the attacker or the malicious actor can capture or record the biometric features or characteristics of the user or the device, such as by using a camera, a scanner, or a microphone, and replay or resend the biometric features or characteristics to the system or the service, as if it was the legitimate or the authentic user or device. The indicator that is generally indicative of a replay attack when dealing with biometric authentication is an exact match, which means that the biometric features or characteristics of the user or the device that are captured or recorded by

the attacker or the malicious actor, and that are replayed or resent to the system or the service, are identical or indistinguishable to the biometric features or characteristics of the user or the device that are stored or registered in the system or the service, and that are used or compared for the authentication or the verification. An exact match can indicate or suggest that the biometric features or characteristics of the user or the device are not genuine or live, but rather fake or replayed, and that the authentication or the verification mechanism or process of the system or the service is compromised or breached by the replay attack.

NEW QUESTION: 725
作為應用程式滲透測試過程的一部分，會話劫持最好透過下列哪一項來實現？
A. 已知明文攻擊
B. 拒口服務 (DoS)
C. Cookie 操作
D. 結構化口詢語言 (SQL) 注入
Answer: (SHOW ANSWER)
Cookie manipulation is a technique that allows an attacker to intercept, modify, or forge a cookie, which is a piece of data that is used to maintain the state of a web session. By manipulating the cookie, the attacker can hijack the session and gain unauthorized access to the web application.
Known-plaintext attack, DoS, and SQL injection are not directly related to session hijacking, although they can be used for other purposes, such as breaking encryption, disrupting availability, or executing malicious commands.

NEW QUESTION: 726
第 2 層隧道協定 (L2TP) 的主要用途是透過隧道傳輸數據
A. 透過會話層的防火牆
B. 透過傳輸層的防火牆
C. 在點對點協定 (PPP) 中
D. 在有效負載壓縮協定 (PCP) 中
Answer: C (LEAVE A REPLY)
The main use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data in the Point-to-Point Protocol (PPP). L2TP is a tunneling protocol that operates at the data link layer (Layer 2) of the OSI model, and is used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. L2TP does not provide encryption or authentication by itself, but it can be combined with IPsec to provide security and confidentiality for the tunneled data. L2TP is commonly used to tunnel PPP sessions over an IP network, such as the Internet. PPP is a protocol that establishes a direct connection between two nodes, and provides authentication, encryption, and compression for the data transmitted over the connection. PPP is often used to connect a remote client to a corporate network, or a user to an ISP. By using L2TP to encapsulate PPP packets, the connection can be extended over a public or shared network, creating a VPN. This way, the user can access the network resources and services securely and transparently, as if they were directly connected to the network.

NEW QUESTION: 727
封裝安全有效載荷(ESP)提供下列哪些功能？
A. 授權與完整性
B. 可用性和完整性
C. 誠信與保密
D. 授權與保密
Answer: C (LEAVE A REPLY)
The Encapsulating Security Payload (ESP) provides integrity and confidentiality for network communications. ESP is a protocol that is part of the IPsec suite, which is a set of protocols and standards that provide security for Internet Protocol (IP) communications. ESP encrypts the payload of an IP packet, which is the data portion of the packet, to provide confidentiality. ESP also adds a trailer and an authentication data field to the packet, to provide integrity. ESP does not provide authorization or availability for network communications. Authorization is the process of granting or denying access to resources based on the identity or role of the requester.
Availability is the property of ensuring that resources are accessible and usable by authorized parties when needed. ESP does not perform authorization or availability functions, but it may support or complement them.

NEW QUESTION: 728
組織實施了保護策略來保護網路免受未經授權的外部存取。新任首席資訊安全長 (CISO) 希望透過更好地保護網路免受未經授權的口部存取來提高安全性。哪種網路存取控制 (NAC) 功能最能滿足此目標？
A. 應用程式防火牆
B. 連接埠安全
C. 強密碼
D. 雙重認證 (2FA)
Answer: B (LEAVE A REPLY)
Port security is a technical control that restricts the access to network ports based on the Media Access Control (MAC) address of the device connected to the port. Port security can prevent unauthorized internal access to the network by preventing rogue devices, such as laptops, smartphones, or USB drives, from connecting to the network through an available port. Port security can also prevent unauthorized external access to the network by preventing devices from bypassing the firewall or other perimeter defenses by connecting directly to an internal port. Port security can also prevent network attacks, such as MAC spoofing, MAC flooding, or ARP poisoning, by limiting the number of MAC addresses allowed on a port or by disabling the port if an unauthorized MAC address is detected.

NEW QUESTION: 729
技術人員正在對客口報告的有關無線效能不佳的問題進行故障排除。使用客口端監視器，技術人員記錄以下資訊：

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

freepdfdumps.com
(ISC)²

下列哪一項最可能是導致該問題的原因？

A. 通道重疊

B. 訊號差

C. 電源設定不正確

D. 天線類型錯誤

Answer: A (LEAVE A REPLY)

The most likely cause of the issue is channel overlap. Channel overlap occurs when multiple wireless access points (WAPs) use the same or adjacent frequency channels, causing interference and degradation of the wireless signal. The image shows that there are four WAPs with the same SSID (Corporate) using channels 9, 10, 11, and 6. These channels are too close to each other and overlap in the 2.4GHz band, resulting in poor wireless performance. The issue can be resolved by changing the channels of the WAPs to non-overlapping ones, such as 1, 6, and 11.

NEW QUESTION: 730

以下哪□最能描述定量□□分析中的“年□生率(ARO)”？

A. □次□□□生□□期造成的全部□□□失

B. □□特定威□在一年内□生的估□□率

C. □次事故中□失的□□价□百分比

D. □施一□控制措施一年的□成本

Answer: (SHOW ANSWER)

ARO represents the estimated number of times a particular risk event is expected to occur within a year. It is combined with the Single Loss Expectancy (SLE) to calculate the Annualized Loss Expectancy (ALE): ALE = SLE ?ARO.

NEW QUESTION: 731

下列哪一項是身份驗證協議，其中每次登入工作階段都會□生一個唯一的新隨機數？

A. 挑戰握手認證協定(CHAP)

B. 點對點協定(PPP)

C. 可擴充身份驗證協定(EAP)

D. 密碼認證協定(PAP)

Answer: A (LEAVE A REPLY)

Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol in which a new random number is generated uniquely for each login session. CHAP is used to authenticate a user or a system over a Point-to-Point Protocol (PPP) connection, such as a dial-up or a VPN connection. CHAP works as follows: The server sends a challenge message to the client, which contains a random

number. The client calculates a response by applying a one-way hash function to the random number and its own secret key, and sends the response back to the server. The server performs the same calculation using the same random number and the secret key stored in its database, and compares the results. If they match, the authentication is successful. CHAP provides more security than Password Authentication Protocol (PAP), which sends the username and password in clear text over the network.

NEW QUESTION: 732
下列哪一項法規規定如何處理資料外洩？
A. 薩班斯奧克斯利法案 (SOX)
B. 美國國家標準與技術研究院 (NIST)
C. 支付卡□業資料安全標準 (PCI-DSS)
D. 一般資料保護規範 (GDPR)
Answer: D (LEAVE A REPLY)
The General Data Protection Regulation (GDPR) is a regulation that dictates how data breaches are handled, among other data protection and privacy requirements. The GDPR applies to any organization that processes the personal data of individuals in the European Union (EU), regardless of the location of the organization. The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". The GDPR requires the organization to notify the supervisory authority of the data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals. The GDPR also requires the organization to notify the affected individuals of the data breach without undue delay, if the breach is likely to result in a high risk to their rights and freedoms.

NEW QUESTION: 733
以下哪□最能描述“出口点数据清理□□”的目的？
A. 假□“□除”命令无需□一步□□即可永久□除所有数据痕迹。
B. 在介□被重新使用、出售或□置之前，通□抽□或□□等技□正式□□数据清除或介□□□□程是否真正有效。
C. 数据加密作□数据清理的替代方案
D. □适用于□□□□，不适用于数字媒体的□理流程
Answer: B (LEAVE A REPLY)
Data sanitization verification involves formally confirming-through methods such as sampling, forensic verification, or third-party certification-that a sanitization or destruction process (such as degaussing or cryptographic erasure) was actually effective in rendering data unrecoverable, rather than simply assuming the process succeeded, before media is repurposed, resold, or disposed of, providing assurance and an audit trail for compliance purposes.

NEW QUESTION: 734
下列哪一種傳輸媒體最能有效防止資料攔截？

A. 微波爐
B. 雙絞線
C. 光纖
D. 同軸電纜
Answer: (SHOW ANSWER)
Fiber optic is the most effective transmission media in preventing data interception, as it uses light signals to transmit data over thin glass or plastic fibers. Fiber optic cables are immune to electromagnetic interference, which means that they cannot be tapped or eavesdropped by external devices or signals. Fiber optic cables also have a low attenuation rate, which means that they can transmit data over long distances without losing much signal strength or quality.
Microwave, twisted-pair, and coaxial cable are less effective transmission media in preventing data interception, as they use electromagnetic waves or electrical signals to transmit data over metal wires or air. These media are susceptible to interference, noise, or tapping, which can compromise the confidentiality or integrity of the data.

NEW QUESTION: 735
下列哪一項標準可確保資訊相對於其對組織的重要性受到保護？
A. 資料對組織高階管理層的價□
B. 法律要求、價□、重要性以及對未經授權的披露或修改的敏感性
C. 由組織總部所在地確定的法律要求
D. 組織利害關係人，分類經管理委員會批准
Answer: (SHOW ANSWER)
Information-classification frameworks (such as ISO/IEC 27001 and common data-classification standards) specify that data should be classified based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification so that stronger protections are applied to more important or sensitive assets.
This multi-factor approach directly ties protection level to how important the information is to the organization's operations, reputation, and compliance posture.

NEW QUESTION: 736
以下哪□最能描述“身份□□”和“其他”之□的区□？
“授□”？
A. □□授予□□源的□□□限；授□□□身份
B. 身份□□□□主体的身份；授□决定主体被允□□行哪些操作
C. □□和授□是同□□
D. 身份□□□适用于用□；授□□适用于系□
Answer: B (LEAVE A REPLY)
Authentication is the process of verifying that a subject is who they claim to be (e.g., via password, token, or biometric). Authorization occurs after successful authentication and determines what resources or actions the authenticated subject is permitted to access or perform.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 737
下列哪一項是減少系統網路攻擊面的最佳選擇？
A. 確保系統上沒有群組帳口
B. 刪除不必要的系統使用者帳口
C. 停用不必要的連接埠和服務
D. 卸載系統上的預設軟體
Answer: C (LEAVE A REPLY)
The best option to reduce the network attack surface of a system is to disable unnecessary ports and services. The network attack surface of a system is the sum of the points or the areas where an attacker can try to enter, access, or exploit the system over the network, using various methods, such as scanning, probing, or attacking. The network attack surface of a system can be reduced by minimizing the exposure and vulnerability of the system to potential attacks, and by enhancing the security and protection of the system against potential attacks. Disabling unnecessary ports and services is an option that can reduce the network attack surface of a system, as it can eliminate or close the unused or unwanted entry points or areas for the attacker, and as it can improve the performance and security of the system.

NEW QUESTION: 738
防止拒口服務 (DoS) 連線的控制已確定可阻止 50% 的攻擊，並且還可將攻擊的影響降低50%。什麼是剩餘風險？
A. 25%
B. 50%
C. 75%
D. 100%
Answer: A (LEAVE A REPLY)
The residual risk is 25% in this scenario. Residual risk is the portion of risk that remains after security measures have been applied to mitigate the risk. Residual risk can be calculated by subtracting the risk reduction from the total risk. In this scenario, the total risk is 100%, and the risk reduction is 75%. The risk reduction is 75% because the control stops 50% of attacks, and reduces the impact of an attack by 50%. Therefore, the residual risk is 100% - 75% = 25%.
Alternatively, the residual risk can be calculated by multiplying the probability and the impact of the remaining risk. In this scenario, the probability of an attack is 50%, and the impact of an attack is 50%.

Therefore, the residual risk is 50% x 50% = 25%. 50%, 75%, and 100% are not the correct answers to the question, as they do not reflect the correct calculation of the residual risk.

NEW QUESTION: 739
下列哪一項是在虛擬系統上實現多個伺服器的最佳方法？
A. 為每個虛擬伺服器實作多種功能，並為每個虛擬伺服器套用相同的安全性設定。
B. 為每個虛擬伺服器實作一項主要功能，並在主機作業系統上套用高安全性設定。
C. 為每個虛擬伺服器實作一項主要功能，並為每個虛擬伺服器套用單獨的安全性設定。
D. 在同一虛擬伺服器中實作多個功能，並對每個功能套用單獨的安全配置。
Answer: C (LEAVE A REPLY)
Virtualization is a technology that enables the creation of multiple virtual servers that run on a single physical server, sharing its resources, such as CPU, memory, disk, or network. The best approach to implement multiple servers on a virtual system is to implement one primary function per virtual server and apply individual security configuration for each virtual server. This approach can enhance the security, performance, and availability of the virtual servers, as it can isolate the functions and resources of each virtual server, prevent interference or conflicts between different functions, and allow for customized and granular security settings and controls for each virtual server. This approach can also facilitate the management, monitoring, and backup of the virtual servers, as it can simplify the identification, configuration, and recovery of each virtual server.

NEW QUESTION: 740
下列哪一項是讓員工為緊急情況做好準備的意識和培訓計畫中最重要的部分？
A. 為普通員工建立緊急聯絡人以獲取資訊
B. 為在復原中發揮直接作用的人員進行業務連續性和災難復原培訓
C. 針對不同受眾設計業務連續性與災難復原培訓計劃
D. 在公司網站上發佈公司業務連續性和災難復原計劃
Answer: C (LEAVE A REPLY)
In an effective awareness and training plan for preparing employees for emergency situations, it's crucial to recognize that different audiences within the organization have different roles, responsibilities, and levels of involvement in business continuity (BC) and disaster recovery (DR) efforts.
Designing training programs tailored to different audiences ensures that employees receive relevant information based on their specific responsibilities. For example:
Executives and decision-makers need high-level strategic training on how to respond during an emergency.
Critical staff members responsible for recovery operations need detailed, role-specific training.
General employees need training on basic emergency procedures (e.g., evacuation, reporting incidents).
By tailoring the content, you ensure that everyone in the organization knows how to act in a crisis, thus increasing the effectiveness of your response during an actual emergency.

NEW QUESTION: 741

以下哪□最能描述“商□□子□件入侵 (BEC) □型：供□商□子□件入侵?
A. 公司高管□子□件□□直接被攻破的攻□
B. 攻□者入侵合法供□商的□子□件□□，并利用□□□向供□商的□□客□□送欺□性□票或付款□更□求，从而利用□有的信任□□关系□行攻□。
C. 一种只□□商家，而不□□其客□的攻□
D. □□□□供□商管理□件漏洞的技□攻□
Answer: B (LEAVE A REPLY)
Vendor Email Compromise is a specific variant of BEC in which an attacker compromises a legitimate vendor's or supplier's actual email account, then uses that trusted, authentic account to send fraudulent invoices, payment details, or payment change requests to the vendor's real customers, making the fraud particularly convincing since it originates from a genuinely compromised, previously trusted business relationship rather than a spoofed address.

NEW QUESTION: 742
應用程式開發中軟體品質保證的目標是
A. 支援高可用性(HA)系統的開發。
B. 促進可信任運算基礎(TCB)系統的創建。
C. 防止創建易受攻擊的應用程式。
D. 鼓勵開發開源應用程式。
Answer: C (LEAVE A REPLY)
The goal of software assurance in application development is to prevent the creation of vulnerable applications. Software assurance is the process of ensuring that the software is designed, developed, and maintained in a secure, reliable, and trustworthy manner. Software assurance involves applying security principles, standards, and best practices throughout the software development life cycle, such as security requirements, design, coding, testing, deployment, and maintenance. Software assurance aims to prevent or reduce the introduction of vulnerabilities, defects, or errors in the software that could compromise its security, functionality, or quality.

NEW QUESTION: 743
從安全角度來看，對於應用程式的輸入必須做出下列哪些假設？
A. 已測試
B. 已記錄
C. 已驗證
D. 不受信任
Answer: D (LEAVE A REPLY)
From a security perspective, input to an application must always be considered untrusted. This assumption is crucial because malicious actors can attempt to manipulate or craft input in ways that exploit vulnerabilities in the application. Treating all input as untrusted helps to ensure that proper security controls-such as input validation, sanitization, and verification-are in place to prevent attacks

like SQL injection, cross-site scripting (XSS), buffer overflows, or other forms of input-based exploitation.

NEW QUESTION: 744
一家醫療機構正在考慮為其員工和患者提供網路存取。下列哪一項是該機構最安全的資料保護解決方案？
A. 公鑰基礎設施(PKI)和數位簽名
B. 受信任的伺服器憑證和密碼
C. 使用者 ID 和密碼
D. 非對稱加密與使用者 ID
Answer: A (LEAVE A REPLY)
Public Key Infrastructure (PKI) is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates and public keys.
Digital signatures are a type of electronic signature that use public key cryptography to verify the authenticity and integrity of a message or document. A health care provider that is considering Internet access for their employees and patients should use PKI and digital signatures as the most secure solution for protection of data, because they provide confidentiality, integrity, authentication, non-repudiation, and accountability for the data exchanged over the Internet.

NEW QUESTION: 745
如果在系統開發生命週期(SDLC)的維護階段發現漏洞，則必須採取下列哪一項措施？
A. 按照原則和設計指南進行更改。
B. 停止應用程序，直到漏洞修復為止。
C. 向口品負責人報告漏洞。
D. 監控應用程式並審口程式碼。
Answer: A (LEAVE A REPLY)
The action that must be taken if a vulnerability is discovered during the maintenance stage in a SDLC is to make changes following principle and design guidelines. Principle and design guidelines are the rules and standards that define the security objectives, requirements, and specifications of the system. They also provide the criteria and methods for evaluating and testing the security of the system. By making changes following principle and design guidelines, the organization can ensure that the vulnerability is fixed in a secure and consistent manner, and that the system maintains its functionality and quality.

NEW QUESTION: 746
一個全球性組織希望將硬體令牌作為遠端存取多因素身份驗證解決方案的一部分。此方案的主要優點是：
A. 令牌註冊的可擴充性。
B. 提高最終使用者的責任感。
C. 它可以防止未經授權的存取。
D. 它簡化了使用者存取管理。
Answer: (SHOW ANSWER)

The primary advantage of implementing hardware tokens as part of a multifactor authentication solution for remote access is that it protects against unauthorized access by requiring the user to possess something (the token) and to know something (the PIN or password) to authenticate.
Hardware tokens are physical devices that generate one-time passwords (OTP) or digital certificates that are used in conjunction with a personal identification number (PIN) or a password to verify the user's identity.

NEW QUESTION: 747
下列哪一項是全碟加密 (FDE) 漏洞的範例？
A. 當使用者通過裝置驗證後，靜態資料已受到損害。
B. 裝置上的資料無法從備份中復原。
C. 當使用者通過裝置驗證時，傳輸中的資料已被洩露
D. 裝置上的資料無法備份。
Answer: (SHOW ANSWER)
Full-disk encryption (FDE) is a security technique that encrypts the entire hard drive of a device or system, protecting the data at rest from unauthorized access, disclosure, or modification.
However, FDE has a vulnerability that data at rest has been compromised when the user has authenticated to the device, which means that once the user enters the correct password or credentials to boot up the device or system, the data on the hard drive is decrypted and accessible to anyone who has physical access to the device or system, such as a thief or an attacker. This vulnerability can be exploited by using cold boot attacks, evil maid attacks, or other methods that target the device or system when it is powered on or in sleep mode.

NEW QUESTION: 748
下列哪一種機制可以最好地防止跨站請求偽造 (CSRF) 攻擊？
A. 參數化資料庫□詢
B. 白名單輸入□
C. 同步會話令牌
D. 使用強密碼
Answer: (SHOW ANSWER)
Cross-Site Request Forgery (CSRF) attacks occur when an attacker tricks a user into performing an unwanted action on a web application where the user is authenticated. This could result in unintended actions such as transferring money, changing account settings, etc.
To prevent CSRF attacks, a synchronized session token (also known as a CSRF token) is one of the most effective mechanisms.
The synchronized session token works by generating a unique token for each user session. This token is included in all requests that modify sensitive data (such as forms or state-changing requests).
When the server receives the request, it checks that the token submitted with the request matches the one stored in the user's session. Since the attacker cannot predict or obtain the user's session token, any unauthorized request made by the attacker will fail, preventing the CSRF attack.

NEW QUESTION: 749
嵌入式設備的哪些領域最常受到攻擊？
A. 應用程式
B. 韌體
C. 協議
D. 實體接口
Answer: B (LEAVE A REPLY)
The area of embedded devices that are most commonly attacked is firmware. Firmware is a type of software that is embedded in a hardware device and controls its basic functions, such as booting, loading, or updating. Firmware is often stored in read-only memory (ROM) or flash memory, which makes it difficult to modify or erase. Firmware can be attacked by exploiting vulnerabilities in the firmware code, design, or configuration, or by injecting malicious code into the firmware update process. Firmware attacks can compromise the security, functionality, or performance of the embedded device, or even render it unusable or inaccessible.

NEW QUESTION: 750
哪种□型的入侵□□系□(IDS)会将□察到的活□与已知的攻□特征□行比□？
A. 基于异常的入侵□□系□
B. 基于□名的入侵□□系□
C. 基于启□式的入侵□□系□
D. 基于行□的入侵□□系□
Answer: B (LEAVE A REPLY)
Signature-based IDS compares network or system activity against a database of known attack patterns (signatures). It is effective against known threats but cannot detect novel or zero-day attacks, unlike anomaly-based systems that establish a baseline of normal behavior and flag deviations.

NEW QUESTION: 751
當必須對系統進行緊急更改時該怎麼辦？
A. 此變更必須在變更控制委員會的下次會議上獲得優先考量。
B. 測試和審核必須迅速完成。
C. 變更必須立即執行，然後提交給變更委員會
D. 變更已執行，並在系統日誌中進行了記錄
Answer: C (LEAVE A REPLY)
In cases of emergency changes, the priority is to address the issue at hand immediately to prevent any potential impacts on the system or organization. After implementing the change, it should then be documented and submitted to the change control board for review and approval post-implementation.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 752
哪個開放系統互連 (OSI) 層最適合傳輸控制協定/網際網路協定 (TCP/IP) 模型中的網路存取層？
A. 傳輸層
B. 資料鏈路與實體層
C. 應用程式層、表示層和會話層
D. 會話層與網路層
Answer: B (LEAVE A REPLY)
The OSI layer(s) that best corresponds to the network access layer in the TCP/IP model is the Data Link and Physical Layers. The network access layer in the TCP/IP model is the lowest layer that provides the functions and the mechanisms for accessing and transmitting the data or the information over the physical network or the medium, such as the cable, the wireless, or the optical fiber. The network access layer in the TCP/IP model corresponds to the Data Link and Physical Layers in the OSI model, because they provide similar functions and mechanisms for accessing and transmitting the data or the information over the physical network or the medium, such as:
The Physical Layer in the OSI model defines and describes the physical characteristics and the specifications of the network or the medium, such as the voltage, the frequency, the modulation, or the connector, and it converts and transmits the data or the information into the electrical, optical, or radio signals, and vice versa.
The Data Link Layer in the OSI model defines and describes the logical characteristics and the specifications of the network or the medium, such as the addressing, the framing, the error detection, or the flow control, and it establishes and maintains the link or the connection between the systems or the devices, and it transfers and receives the data or the information in the form of the frames or the packets.

NEW QUESTION: 753
下列哪一項是確保遠端使用者使用的端點裝置在允許進入網路之前符合組織核准的策略的最有效方法？
A. 群組原則物件 (GPO)
B. 網路存取控制 (NAC)
C. 行動裝置管理 (MDM)
D. 特權存取管理 (PAM)
Answer: B (LEAVE A REPLY)
The most effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network is to use Network Access Control (NAC). NAC is a security technique that involves verifying and enforcing the compliance of the endpoint

devices with the security policies and standards of the organization, before granting them access to the network. NAC can check the attributes and characteristics of the endpoint devices, such as device type, operating system, IP address, MAC address, or user identity, and compare them with the predefined criteria and rules. NAC can also perform the network access authentication and authorization, and the network health and compliance checks, such as antivirus, firewall, or patch status. NAC can help to ensure the endpoint devices used by remote users are compliant with an organization's approved policies, as it can prevent or restrict the access of any non-compliant or unauthorized endpoint devices, and reduce the security risks and vulnerabilities of the network.

NEW QUESTION: 754
下列哪一種加密技術能口充當串流密碼？
A. 密碼回饋 (CFB)
B. Feistel 密碼
C. 帶有錯誤傳播的密碼塊連結 (CBC)
D. 電子密碼本 (ECB)
Answer: A (LEAVE A REPLY)
Cipher Feedback (CFB) is an encryption technology that has the ability to function as a stream cipher. A stream cipher is a type of symmetric encryption that encrypts or decrypts one bit or byte of plaintext or ciphertext at a time, using a keystream that is derived from a secret key and an initialization vector. CFB is a mode of operation that converts a block cipher, such as AES or DES, into a stream cipher, by feeding the output of the block cipher back into its input, and XORing it with the plaintext or ciphertext. CFB can provide the advantages of both block ciphers and stream ciphers, such as high security, low error propagation, and high efficiency. Feistel cipher, Cipher Block Chaining (CBC) with error propagation, and Electronic Code Book (ECB) are not encryption technologies that have the ability to function as stream ciphers. These are types of block ciphers or modes of operation that encrypt or decrypt a fixed-length block of plaintext or ciphertext at a time, using a secret key and a chaining mechanism. Block ciphers are different from stream ciphers in terms of their design, operation, and performance.

NEW QUESTION: 755
一個組織正在實施安全審口作為系統開發的一部分。下列哪一項是最好遵循的技術？
A. 聘請第三方審計公司。
B. 檢討安全架構。
C. 執行增量評估。
D. 進行滲透測試。
Answer: C (LEAVE A REPLY)
The best technique to follow when implementing security review as part of system development is to perform incremental assessments. Security review is the process of evaluating and verifying the security requirements, design, implementation, and testing of a system. Security review aims to identify and mitigate the security risks and vulnerabilities of the system, and to ensure that the system meets

the security standards and best practices. Security review should be performed as part of system development, which is the process of creating or modifying a system. System development follows a life cycle model, such as waterfall, agile, or spiral, that defines the phases and activities of the system development process. Security review should be performed incrementally, which means that security review should be conducted at each phase and activity of the system development life cycle, and not only at the end of the system development process.
Performing incremental assessments can provide the following benefits:
It can reduce the cost and complexity of security review, as the security issues and defects can be detected and fixed early in the system development process, rather than later when they are more expensive and difficult to resolve.
It can improve the quality and effectiveness of security review, as the security review can be tailored and aligned with the specific objectives and deliverables of each phase and activity of the system development process, rather than using a generic or one-size-fits-all approach.
It can enhance the security and performance of the system, as the security review can ensure that the security requirements and controls are integrated and implemented throughout the system development process, rather than added or patched as an afterthought.

NEW QUESTION: 756
一家從消費者收集資訊的大型國際組織已與軟體即服務 (SaaS) 雲端供應商簽訂合約來處理這些資料。SaaS 雲端供應商使用額外的資料處理來展示其希望向資料擁有者提供的其他功能。該供應商認為允許進行額外的數據處理活動，因為他們沒有向其他組織披露 下列哪一項最能支持這個理由？
A. 資料始終加密，只有少數雲端提供者員工可以存取。
B. 身為資料擁有者，雲端提供者有權指示如何處理資料。
C. 身為資料處理者，雲端提供者有權決定如何處理資料。
D. 雙方之間的協議含糊不清，沒有詳細□明如何使用數據
Answer: (SHOW ANSWER)
The large org is the data controller and CSP is its data processor. But data processors do not decide how to process data. Data Controller, the large org controls how data is to be processed.

NEW QUESTION: 757
以下哪□最能描述数字取□中的“□据□”概念？
A. □据□□的□序
B. 一份完整、□□的□□，□□□□了从收集到呈堂□程中，□在何□何地在何种情况下□理了□据。
C. □□□□中法医分析□的□□
D. 适用于□□□据的分□□□
Answer: B (LEAVE A REPLY)
Chain of custody is the chronological, documented record showing the collection, transfer, handling, and storage of evidence, ensuring its integrity and admissibility in legal proceedings by proving that the evidence was not altered or tampered with at any point.

NEW QUESTION: 758
駭客可以使用鎖定功能來發動下列哪一種攻擊？
A. 拒□服務（DoS）
B. 字典
C. Ping 洪水攻擊
D. 中間人（MITM）
Answer: (SHOW ANSWER)
A denial of service (DoS) attack is an attempt to prevent legitimate users from accessing a service or a resource by overwhelming it with malicious traffic or requests. A hacker can use a lockout capability to start a DoS attack by repeatedly sending invalid authentication attempts to a system or an application that has a policy of locking out accounts after a certain number of failed attempts. This can result in locking out legitimate users from accessing the system or the application, or consuming the system's resources and slowing down its performance. A dictionary attack is a type of brute force attack that tries to guess passwords or encryption keys by using a list of common or likely words. A ping flood attack is a type of DoS attack that sends a large number of ping packets to a target system, hoping to consume its bandwidth or processing power. A man-in-the-middle (MITM) attack is a type of attack that intercepts and alters the communication between two parties, without their knowledge or consent.

NEW QUESTION: 759
以下哪□最能描述 PBKDF2、bcrypt 或 Argon2 等“密□拉伸”技□的目的？
A. 自□生成更□的加密密□
B. 故意增加从密□推□出密□所需的□算量，从而减□暴力破解攻□。
C. □了提高存□效率而□□加密密□。
D. 用于在分布式系□中同步加密密□
Answer: (SHOW ANSWER)
Key stretching algorithms intentionally introduce computational or memory-intensive work (via multiple iterations or memory-hard functions) when deriving a cryptographic key from a password, significantly increasing the time and resources required for brute-force or dictionary attacks against stored password hashes.

NEW QUESTION: 760
應如何定義組織社群媒體□容的保留期限？
A. 透過每個社群媒體服務的保留政策
B. 根據組織的記錄保留政策
C. 由資訊長 (CIO) 撰寫
D. 按可用儲存空間量
Answer: B (LEAVE A REPLY)
The retention period for an organization's social media content should be determined by the organization's records retention policy, which outlines how long various types of records (including digital content like social media posts) should be kept before being disposed of. This policy is usually based on factors such as:

Legal and regulatory requirements: There may be laws that specify how long certain types of records must be retained (e.g., financial records, contracts, communications).
Business needs: Content might be kept for operational purposes, such as marketing analysis, customer engagement, or historical record-keeping.
Security and privacy considerations: The organization may choose to delete content after a certain period to minimize the risk of data exposure.
By aligning the retention period for social media content with the organization's records retention policy, the organization ensures that content is managed consistently across all channels and in accordance with relevant laws and best practices.

NEW QUESTION: 761
在考慮實施軟體定義網路 (SDN) 時，安全性問題是什麼？
A. 它增加了攻擊足跡。
B. 它使用開源協定。
C. 它有分散式架構。
D. 它是基於雲端的。
Answer: (SHOW ANSWER)
A security concern when considering implementing software-defined networking (SDN) is that it increases the attack footprint. SDN is a network architecture that decouples the control plane from the data plane, and centralizes the network intelligence and management in a software controller. SDN enables more flexibility, scalability, and programmability of the network, as well as better integration with cloud services and applications. However, SDN also introduces new security challenges and risks, such as the following:
It increases the attack footprint, as the SDN controller becomes a single point of failure and a high-value target for attackers. If the SDN controller is compromised, the attacker can gain access to the entire network and manipulate its behavior or performance.
It exposes new attack vectors, as the SDN controller communicates with the network devices and applications via open and standardized protocols, such as OpenFlow, REST, or NETCONF.
These protocols may have vulnerabilities or weaknesses that could be exploited by attackers to launch denial-of-service, man-in-the-middle, or spoofing attacks.
It requires more trust and verification, as the SDN controller relies on the information and feedback from the network devices and applications to make decisions and enforce policies. The network devices and applications may provide inaccurate or malicious information to the SDN controller, or may not comply with the instructions or configurations from the SDN controller, leading to security breaches or inconsistencies.

NEW QUESTION: 762
下列哪項措施用於確保資料探勘活動不會洩漏敏感資料？
A. 在底層基礎設施上實施雙重認證。
B. 對欄位層級資料進行加密，並嚴格控制加密金鑰

C. 對資料庫進行預處理，以口看是否可以從學習到的模式中揭示資訊。
D. 對資料元素實施最小權限原則，以便減少可以存取資料庫的使用者數量。
Answer: (SHOW ANSWER)
Encrypting data at the field level ensures that sensitive information remains confidential and secure even during data mining activities. Tight control over encryption keys further ensures that only authorized personnel can access and decrypt sensitive data.

NEW QUESTION: 763
使用密文和由此口生的明文訊息來導出非字母密鑰是哪種密碼分析攻擊方法的範例？
A. 頻率分析
B. 純密文攻擊
C. 可能的明文攻擊
D. 已知明文攻擊
Answer: D (LEAVE A REPLY)
A known-plaintext attack is a type of cryptanalytic attack where the attacker has access to both the ciphertext and the corresponding plaintext, and tries to derive the key or the algorithm used to encrypt the message. This type of attack can be effective against some symmetric ciphers, such as substitution ciphers, where the key is non-alphabetic and the ciphertext is a permutation of the plaintext. For example, if the attacker knows that the plaintext "HELLO" corresponds to the ciphertext "QNUUX", they can infer that the key is "Q-H, N-E, U-L, X-O". A frequency analysis attack is a type of cryptanalytic attack where the attacker analyzes the frequency of letters or symbols in the ciphertext and compares them with the expected frequency of the language of the plaintext. A ciphertext-only attack is a type of cryptanalytic attack where the attacker only has access to the ciphertext and tries to guess the plaintext or the key by using statistical methods, brute force, or other techniques. A probable-plaintext attack is a type of cryptanalytic attack where the attacker has access to the ciphertext and some information about the probable plaintext, such as the format, the length, or some common words or phrases, and tries to recover the key or the algorithm used to encrypt the message.

NEW QUESTION: 764
根據美國國家標準與技術研究所 (NIST) 的口法，下列哪一個目標代表了風險管理的現代轉變？
A. 重點在於不斷變化、不斷發展且充滿新威脅的操作環境。
B. 儲存、處理或傳輸組織資訊的安全資訊技術 (IT) 系統。
C. 使管理階層能口做出基於風險的明智決策，證明安全支出的合理性。
D. 提供改進的任務完成方法。
Answer: A (LEAVE A REPLY)
The goal that represents a modern shift in risk management according to National Institute of Standards and Technology (NIST) is to focus on operating environments that are changing, evolving, and full of emerging threats. Risk management is the process that involves identifying, assessing, and prioritizing the risks that affect an organization or a system, and applying the appropriate strategies and actions to mitigate or reduce the risks, and to achieve the objectives and goals of the organization or

the system. NIST is a federal agency that develops and publishes standards, guidelines, and best practices for various fields, including information security and risk management. NIST has proposed a modern shift in risk management, which is to focus on operating environments that are changing, evolving, and full of emerging threats, rather than on static or fixed environments that are assumed to be stable or predictable. This modern shift in risk management recognizes the dynamic and complex nature of the current and future operating environments, and the need for adaptive and resilient risk management approaches that can respond to the changing and evolving risks and opportunities.

NEW QUESTION: 765
開發團隊的任務是從生物辨識設備收集資料。該應用程式將支援各種收集資料流。在測試階段，團隊在安全的測試環境中利用舊生口資料庫中的資料。
團隊考慮了什麼原則？
A. 生物辨識資料無法變更。
B. 單獨的生物辨識資料流需要更高的安全性。
C. 生物辨識設備未知。
D. 必須保護生物辨識資料免於外洩。
Answer: D (LEAVE A REPLY)
By utilizing data from an old production database in a secure testing environment, the team is likely taking steps to protect biometric data from unauthorized access or exposure during the testing phase. Testing with this kind of data in a secure environment ensures that sensitive biometric data remains protected and is not disclosed to anyone who shouldn't have access to it, while still allowing the development and testing process to proceed effectively.

NEW QUESTION: 766
請參考以下資訊來回答問題。
一名新員工獲得一台具有完全管理員存取權限的筆記型電腦。
該員工家裡沒有個人計算機，但有一個孩子使用電腦發送和接收電子郵件, 搜尋網路和使用即時訊息。
該組織的資訊技術 (IT) 部門發現使用員工的存取權限在電腦上安裝了點對點程式。
下列哪一種方法是從電腦中刪除點對點 (P2P) 程式最有效的方法？
A. 運行軟體卸載
B. 重新映像計算機
C. 尋找並刪除所有安裝文件
D. 刪除網頁瀏覽器快取中儲存的所有 cookie
Answer: B (LEAVE A REPLY)
The most effective way of removing the P2P program from the computer is to re-image the computer. Re-imaging the computer means to restore the computer to its original or desired state, by erasing or overwriting the existing data or software on the computer, and by installing a new or a backup image of the operating system and the applications on the computer. Re-imaging the computer can ensure that the P2P program and any other unwanted or harmful programs or files are completely removed from the computer, and that the computer is clean and secure. Run software uninstall, find and remove all

installation files, and delete all cookies stored in the web browser cache are not the most effective ways of removing the P2P program from the computer, as they may not remove all the traces or components of the P2P program from the computer, or they may not address the other potential issues or risks that the P2P program may have caused on the computer.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 767
下列哪一項是光纖通訊的常見風險？
A. 資料發射，在可行的情況下部署6 類及更高等級的電纜
B. 漏光，盡可能部署屏蔽電纜
C. 電纜損壞，盡可能部署環形架構
D. 電子竊聽，在可行的情況下部署端對端加密
Answer: (SHOW ANSWER)
Light leakage is a common risk with fiber optical communications, as it may allow an attacker to intercept or modify the data transmitted through the fiber cable. Light leakage may occur due to bends, cracks, or splices in the cable, or due to improper termination or connection of the cable.
The associated mitigation measure for light leakage is to deploy shielded cable wherever feasible, as it can reduce the amount of light escaping from the cable and prevent external interference. Data emanation is not a risk with fiber optical communications, as it is a phenomenon that affects electrical signals, not optical signals. Cable damage is a risk with any type of cable, not specific to fiber optical communications. Electronic eavesdropping is not a risk with fiber optical communications, as it involves capturing the electromagnetic emissions from a device, not the optical signals from a cable.

NEW QUESTION: 768
最近的一項資訊安全風險評估將行動裝置上的系統存取控制薄弱視為一個嚴重問題。
A. 入侵防禦系統 (IPS)
B. 多重驗證 (MFA)
C. 資料遺失保護 (DLP)
D. 靜態資料加密
Answer: B (LEAVE A REPLY)
Multi-factor authentication (MFA) is a method of authentication that requires two or more independent factors to verify the identity of a user, such as something you know, something you have, or something you are. MFA can help address the risk of weak system access controls on mobile devices, as it provides a higher level of security than a single factor, such as a password.

MFA can prevent unauthorized access to company information, even if the mobile device is lost, stolen, or compromised. An intrusion prevention system (IPS) is a device or software that monitors and blocks network traffic based on predefined rules or signatures. An IPS can help protect the network from external attacks, but it does not address the system access controls on mobile devices. Data loss protection (DLP) is a system or tool that prevents the unauthorized disclosure, transfer, or leakage of sensitive data. DLP can help protect the company information from being exposed, but it does not address the system access controls on mobile devices. Data at rest encryption is a technique that encrypts the data that is stored on a device or a media. Data at rest encryption can help protect the company information from being accessed, even if the mobile device is lost, stolen, or compromised, but it does not address the system access controls on mobile devices.

NEW QUESTION: 769
下列哪一項有助於識別電腦上執行的惡意軟體的來源網際網路通訊協定 (IP) 位址？
A. 開口的網路連線列表
B. 顯示傳輸控制協定/Internet 協定 (TCP/IP) 網路設定資訊。
C. 正在執行的進程列表
D. 顯示位址解析協定 APP）表
Answer: A (LEAVE A REPLY)
The tool that will help identify the source IP address of malware being executed on a computer is the list of open network connections. The list of open network connections is a tool that displays the active network connections on a computer, such as the TCP or UDP sockets, the local and remote IP addresses and ports, the process ID and name, and the connection state. The list of open network connections can be obtained by using commands such as netstat, lsof, or ss, depending on the operating system. The list of open network connections can help identify the source IP address of malware being executed on a computer, by showing the suspicious or malicious network activity that the malware may generate, such as connecting to a command and control server, downloading or uploading data, or scanning for vulnerabilities. The list of open network connections can also help identify the process name and ID of the malware, which can be further investigated by using other tools, such as the list of running processes or the display of the Address Resolution Protocol (ARP) table.

NEW QUESTION: 770
當網路管理外包給第三方時，下列何者是保護關鍵資料資口最有效的方法？
A. 記錄與敏感系統相關的所有活動
B. 提供安全策略的鏈接
C. 確認已簽署保密協議
D. 採用嚴格的存取控制
Answer: D (LEAVE A REPLY)
When network management is outsourced to third parties, strong access controls are the most effective method of protecting critical data assets. Access controls define who can access what data and what

actions they can perform, ensuring that only authorized personnel (whether internal or from the third party) can access sensitive data and systems.
Key points about strong access controls:
Limit access: Ensure that third-party personnel only have access to the systems, applications, and data they need to perform their tasks. This is typically done through role-based access control (RBAC), least privilege principles, and segregation of duties.
Authentication: Use strong authentication methods (e.g., multi-factor authentication) to verify the identity of individuals accessing sensitive data.
Monitoring and auditing: Regularly monitor and audit access to critical systems to detect unauthorized access or suspicious activities.
This approach is essential because third-party network managers will need some level of access to your systems, and strong access controls help mitigate the risk of unauthorized access, data breaches, or insider threats.

NEW QUESTION: 771
某組織經營著一套老舊的工業控制系統 (ICS) 來支援其核心業務服務，該系統即將被取代 其管理必須透過管理控制台軟體進行遠端執行，而該軟體又依賴一個已知易受多種攻擊的舊版Java 執行時間環境 (JPE)。如何才能最好地管理這種風險？
A. 將整個 ICS 隔離到其自身的網路段上
B. 對用於管理目的的主機進行氣隙隔離和加固
C. □服管理階層停用工業控制系統 (ICS) 並過渡到現代技術
D. 在所有客□端和易受攻擊的管理站之間部署限制性代理程式。
Answer: (SHOW ANSWER)
Air-gapping and hardening the host used for management purposes is the best way to manage the risk of a legacy Industrial Control System (ICS) that depends on a vulnerable version of the Java Runtime Environment (JRE). Air-gapping means disconnecting the host from any network or internet connection, so that it can only be accessed physically. Hardening means applying security patches, disabling unnecessary services, and configuring security settings to reduce the attack surface of the host. This way, the risk of remote exploitation of the JRE vulnerability is minimized, and the host is protected from other potential threats. Isolating the full ICS by moving it onto its own network segment may reduce the exposure of the system, but it does not eliminate the possibility of network- based attacks. Convincing the management to decommission the ICS and migrate to a modern technology may be the ideal solution, but it may not be feasible or cost- effective, especially if the ICS cannot be replaced. Deploying a restrictive proxy between all clients and the vulnerable management station may also help to filter and monitor the network traffic, but it does not address the root cause of the vulnerability, and it may introduce additional complexity and overhead to the system.

NEW QUESTION: 772
在□估身份即服□ (IDaaS) 解决方案□，以下哪份□告能□提供最□尽的控制措施□明？
A. □□准□公告(SAS)70
B. 服□□□控制(SOC)2

C. 服□□□控制(SOC)3
D. 服□□□控制(SOC)1
Answer: (SHOW ANSWER)

NEW QUESTION: 773
在處理即時虛擬化環境中的進階持續性威脅 (APT) 入侵時，下列哪一種技術最有用？
A. 防毒操作
B. 逆向工程
C. □存取證
D. 日誌檔分析
Answer: C (LEAVE A REPLY)
Memory forensics is the most useful technique when dealing with Advanced Persistent Threat (APT) intrusions on live virtualized environments. Memory forensics is the analysis of the volatile memory of a system, such as RAM, cache, or registers. Memory forensics can reveal valuable information about the state and activities of the system, such as running processes, open files, network connections, encryption keys, malware signatures, and user credentials. Memory forensics is especially useful for detecting and investigating APTs, which are stealthy and persistent attacks that often evade traditional security measures and leave little or no traces on the disk.

NEW QUESTION: 774
某個組織的首席資訊安全長 (CISO) 要求建立一份服務組織控制 (SOC) 報告，以概述特定係統在12 個月期間的安全性和可用性。應使用哪種類型的 SOC 報告？
A. SOC 1 類型 1
B. SOC 2 類型 2
C. SOC 2 類型 2
D. SOC 3 類型 1
Answer: B (LEAVE A REPLY)
The type of SOC report that should be utilized to outline the security and availability of a particular system over a 12-month period is SOC 2 Type 2. SOC 2 Type 2 is a security audit report that provides information about the design and the operating effectiveness of the controls at a service organization relevant to the security and availability trust service categories, as well as the other trust service categories such as processing integrity, confidentiality, and privacy. SOC 2 Type 2 is the type of SOC report that should be utilized to outline the security and availability of a particular system over a 12-month period, because it can:
Evaluate and assess the design and the effectiveness of the controls that the service organization has implemented and maintained for ensuring the security and availability of the system and the data that are used for providing the services or the solutions to the user entities or the customers, based on the criteria or the principles of the Trust Services Categories (TSC).
Provide and present the information and the data about the service organization's system and the controls in relation to the security and availability, in the form of the audit report or the opinion that is

prepared and issued by the independent auditor or the practitioner, and that is intended for the general or the restricted use of the user entities and the other interested or relevant parties or stakeholders. Cover a specified period of time, usually between six and twelve months, and include the description of the tests of controls and the results performed by the auditor, to demonstrate the operational effectiveness of the controls over the security and availability of the system and the data.

NEW QUESTION: 775
路由器在哪對開放系統互連 (OSI) 參考模型層之間用作通訊設備？
A. 傳輸和會話
B. 資料鏈路與傳輸
C. 網路和會話
D. 物理和資料鏈路
Answer: C (LEAVE A REPLY)
Routers operate at the Network Layer (Layer 3), where they forward packets based on IP addresses. They do not interact directly with the Session Layer (Layer 5).

NEW QUESTION: 776
一位安全顧問受邀研究某組織在保護隱私相關資訊方面的法律義務。哪種類型的口讀材料與此項目最相關？
A. 該組織目前關於隱私問題的安全政策
B. 適用於該組織的監管機構強制執行的隱私相關法規
C. 由公認的安全標準組織發布的隱私最佳實踐
D. 旨在保護隱私資訊的組織程序
Answer: (SHOW ANSWER)
The most relevant reading material for researching an organization's legal obligations to protect privacy-related information is the privacy-related regulations enforced by governing bodies applicable to the organization. These regulations define the legal requirements, standards, and penalties for collecting, processing, storing, and disclosing personal or sensitive information of individuals or entities. The organization must comply with these regulations to avoid legal liabilities, fines, or sanctions.

NEW QUESTION: 777
下列哪一項可確保舊日誌資料不被覆蓋？
A. 增加日誌檔案大小
B. 實施系統日誌
C. 日誌保存
D. 日誌保留
Answer: (SHOW ANSWER)
Log retention is the process of keeping old log data for a certain period of time before deleting or archiving it. Log retention ensures that old log data is not overwritten by new log data, which could result in the loss of valuable information or evidence. Log retention also helps to comply with legal or regulatory requirements, such as the GDPR, that may mandate the retention of log data for a specific

duration. Log retention can be implemented by using policies, procedures, and tools that define how long and where to store log data, how to protect log data from unauthorized access or modification, and how to dispose of log data securely when it is no longer needed.

NEW QUESTION: 778
安全架構師計劃參考強制存取控制 (MAC) 模型進行實作。這顯示下列哪些屬性被優先考慮？
A. 保密性
B. 誠信
C. 可用性
D. 輔助功能
Answer: A (LEAVE A REPLY)
According to the CISSP Official (ISC)2 Practice Tests, the property that is prioritized by a Mandatory Access Control (MAC) model for implementation is confidentiality. Confidentiality is the property that ensures that the data or information is only accessible or disclosed to the authorized parties, and is protected from unauthorized or unintended access or disclosure. A MAC model is a type of access control model that grants or denies access to an object based on the security labels of the subject and the object, and the security policy enforced by the system. A security label is a tag or a marker that indicates the classification, sensitivity, or clearance of the subject or the object, such as top secret, secret, or confidential. A security policy is a set of rules or criteria that defines how the access decisions are made based on the security labels, such as the Bell-LaPadula model or the Biba model. A MAC model prioritizes confidentiality, as it ensures that the data or information is only accessible or disclosed to the subjects that have the appropriate security labels and clearance, and that the data or information is not leaked or compromised by the subjects that have lower security labels or clearance. Integrity is not the property that is prioritized by a MAC model for implementation, although it may be a property that is supported or enhanced by a MAC model. Integrity is the property that ensures that the data or information is accurate, complete, and consistent, and is protected from unauthorized or unintended modification or corruption. A MAC model may support or enhance integrity, as it ensures that the data or information is only modified or corrupted by the subjects that have the appropriate security labels and clearance, and that the data or information is not altered or damaged by the subjects that have lower security labels or clearance. However, a MAC model does not prioritize integrity, as it does not prevent or detect the modification or corruption of the data or information by the subjects that have the same or higher security labels or clearance, or by the external factors or events, such as errors, failures, or accidents. Availability is not the property that is prioritized by a MAC model for implementation, although it may be a property that is supported or enhanced by a MAC model. Availability is the property that ensures that the data or information is accessible and usable by the authorized parties, and is protected from unauthorized or unintended denial or disruption of access or use. A MAC model may support or enhance availability, as it ensures that the data or information is accessible and usable by the subjects that have the appropriate security labels and clearance, and that the data or information is not denied or disrupted by the subjects that have lower security labels or clearance. However, a MAC model does not prioritize availability, as it does not prevent or detect the denial or disruption of access or use of the data or information by the subjects that have the same or

higher security labels or clearance, or by the external factors or events, such as attacks, failures, or disasters. Accessibility is not the property that is prioritized by a MAC model for implementation, as it is not a security property, but a usability property. Accessibility is the property that ensures that the data or information is accessible and usable by the users with different abilities, needs, or preferences, such as the users with disabilities, impairments, or limitations. Accessibility is not a security property, as it does not protect the data or information from unauthorized or unintended access, disclosure, modification, corruption, denial, or disruption. Accessibility is a usability property, as it enhances the user experience and satisfaction of the data or information.

NEW QUESTION: 779
在通用標準中，下列哪一項是表達一組獨立於實現的安全要求的正式文件？
A. 組織安全策略
B. 安全目標 (ST)
C. 保護設定檔 (PP)
D. 評估目標 (TOE)
Answer: C (LEAVE A REPLY)
The common criteria is an international standard for evaluating the security and assurance of information technology products and systems. It defines a common framework and language for specifying, implementing, and evaluating security requirements and functions. In the common criteria, a Protection Profile (PP) is a formal document that expresses an implementation- independent set of security requirements for a category of products or systems that share a common security problem or objective. A PP defines the security problem, the security objectives, the security functional requirements, and the security assurance requirements for the intended products or systems. A PP can be used by customers, developers, or evaluators as a basis for selecting, developing, or evaluating security solutions.

NEW QUESTION: 780
下列哪一項最能代表最小特權的概念？
A. 除非明確允許訪問，否則拒口對物件的存取。
B. 只有擁有者才能存取物件。
C. 允許存取對象，除非該對象受資訊安全性原則保護。
D. 僅允許透過存取控制清單 (ACL) 進行驗證的使用者存取物件。
Answer: (SHOW ANSWER)
According to the CISSP CBK Official Study Guide, the concept of least privilege means that users and processes should only have the minimum access required to perform their tasks, and no more. This reduces the risk of unauthorized or malicious actions, as well as the impact of potential incidents. One way to implement the principle of least privilege is to use a default-deny policy, which means that access to an object is denied unless access is specifically allowed. This is also known as a whitelist approach, which only grants access to predefined and authorized entities. Access to an object is only available to the owner is not a good representation of the concept of least privilege, as it may prevent legitimate access by other authorized users or processes. Access to an object is allowed unless it is

protected by the information security policy is not a good representation of the concept of least privilege, as it may allow unnecessary or excessive access by default. This is also known as a blacklist approach, which only denies access to predefined and unauthorized entities. Access to an object is only allowed to authenticated users via an Access Control List (ACL) is not a good representation of the concept of least privilege, as it may not consider the authorization and accountability aspects of access control. Authentication is the process of verifying the identity of a user or process, while authorization is the process of granting or denying access based on the identity and the access policy. An ACL is a mechanism that defines the permissions and restrictions for accessing an object, but it does not necessarily enforce the principle of least privilege.

NEW QUESTION: 781
以下哪□最能描述“出口点数据□失防□与端点□□和响□ (EDR) 集成”的目的？
A. 完全取代基于网□的DLP需求
B. 将端点□活□(例如文件□□和□程行□)与数据移□事件关□起来，从而更全面地了解源自端点或途□端点的潜在数据泄露情况。
C. □□用于管理□端硬件清□
D. 自□加密所有□端硬□
Answer: B (LEAVE A REPLY)
Integrating DLP with EDR allows security teams to correlate endpoint-level activity-such as which process accessed a sensitive file or attempted to copy it to removable media-with broader data movement events, providing more complete visibility into potential data exfiltration attempts that originate from or pass through an endpoint, rather than relying solely on network-level DLP visibility.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 782
至少應安排個人或群組帳□的權限審核
A. 每年
B. 與員工晉升相對應
C. 與終止相對應
D. 持續
Answer: D (LEAVE A REPLY)
The minimum frequency for audits of permissions to individual or group accounts is continually. Audits of permissions are the processes of reviewing and verifying the user accounts and access rights on a system or a network, and ensuring that they are appropriate, necessary, and compliant with the

policies and standards. Audits of permissions can provide some benefits for security, such as enhancing the accuracy and the reliability of the user accounts and access rights, identifying and removing any excessive, obsolete, or unauthorized access rights, and supporting the audit and the compliance activities. Audits of permissions should be performed continually, which means that they should be conducted on a regular and consistent basis, without any interruption or delay. Continual audits of permissions can help to maintain the security and the integrity of the system or the network, by detecting and addressing any changes or issues that may affect the user accounts and access rights, such as role changes, transfers, promotions, or terminations. Continual audits of permissions can also help to ensure the effectiveness and the feasibility of the audit process, by reducing the workload and the complexity of the audit tasks, and by providing timely and relevant feedback and results. Annually, to correspond with staff promotions, and to correspond with terminations are not the minimum frequencies for audits of permissions to individual or group accounts, although they may be related or possible frequencies. Annually means that the audits of permissions are performed once a year, which may not be sufficient or adequate to maintain the security and the integrity of the system or the network, as the user accounts and access rights may change or become outdated more frequently than that, due to various factors, such as role changes, transfers, promotions, or terminations. Annually audits of permissions may also increase the workload and the complexity of the audit process, as they may involve a large number of user accounts and access rights to review and verify, and they may not provide timely and relevant feedback and results. To correspond with staff promotions means that the audits of permissions are performed whenever a staff member is promoted to a higher or a different position within the organization, which may affect their user accounts and access rights. To correspond with staff promotions audits of permissions can help to ensure that the user accounts and access rights are aligned with the current roles or functions of the staff members, and that they follow the principle of least privilege. However, to correspond with staff promotions audits of permissions may not be sufficient or adequate to maintain the security and the integrity of the system or the network, as the user accounts and access rights may change or become outdated due to other factors, such as role changes, transfers, or terminations, and they may not be performed on a regular and consistent basis. To correspond with terminations means that the audits of permissions are performed whenever a staff member leaves the organization, which may affect their user accounts and access rights. To correspond with terminations audits of permissions can help to ensure that the user accounts and access rights are revoked or removed from the system or the network, and that they prevent any unauthorized or improper access or use. However, to correspond with terminations audits of permissions may not be sufficient or adequate to maintain the security and the integrity of the system or the network, as the user accounts and access rights may change or become outdated due to other factors, such as role changes, transfers, or promotions, and they may not be performed on a regular and consistent basis.

NEW QUESTION: 783

以下哪□最能描述“加密擦除”(加密粉碎)作□一种数据清除方法？

A. 通□粉碎的方式物理□□存□介□

B. 通□安全地□除或□□用于保□加密数据的加密密□，使加密数据永久无法恢复，而不是覆盖或物理□□底□存□介□本身。
C. 使用随机模式多次覆盖数据
D. 一种□适用于未加密数据的方法
Answer: B (LEAVE A REPLY)
Cryptographic erasure (crypto-shredding) renders previously encrypted data permanently unrecoverable by securely deleting or destroying the encryption key used to protect it, rather than overwriting or physically destroying the underlying storage media itself. Since the data remains encrypted and the key is irrecoverably gone, the data is effectively rendered inaccessible-a particularly efficient sanitization method for large volumes of data or media that will be reused, such as in cloud environments where physical destruction is often impractical.

NEW QUESTION: 784
攻擊模擬和威脅分析 (PASTA) 的威脅建模使用流程是什麼？
A. 應用分解、威脅分析、漏洞偵測、攻擊枚舉、風險/影響分析
B. 威脅分析、漏洞偵測、應用程式分解、攻擊枚舉、風險/影響分析
C. 風險/影響分析、應用分解、威脅分析、漏洞偵測、攻擊枚舉
D. 應用分解、威脅分析、風險/影響分析、漏洞偵測、攻擊枚舉
Answer: (SHOW ANSWER)
Application decomposition, threat analysis, vulnerability detection, attack enumeration, risk/impact analysis is the threat modeling order using Process for Attack Simulation and Threat Analysis (PASTA). PASTA is a risk-centric threat modeling methodology that aims to identify and prioritize the most likely and impactful threats and vulnerabilities for a given system or application. PASTA consists of seven stages: definition, application decomposition, threat analysis, vulnerability analysis, attack enumeration, risk/impact analysis, and countermeasure selection. In each stage, PASTA uses various techniques and tools, such as data flow diagrams, attack trees, threat libraries, vulnerability scanners, risk matrices, and security controls, to perform a comprehensive and realistic threat assessment and mitigation plan.

NEW QUESTION: 785
下列哪一項是最有效的糾正控制措施，可以最大限度地減少物理入侵的影響？
A. 對可能的入侵進行自動錄影
B. 警衛或警察快速反應以逮捕可能的入侵者
C. □動明亮的燈光以嚇跑可能的入侵者
D. 發出響亮的警報以嚇跑可能的入侵者
Answer: B (LEAVE A REPLY)
A rapid response by guards or police to apprehend a possible intruder is the most effective corrective control to minimize the effects of a physical intrusion. A corrective control is a type of security control that aims to restore the normal operations and security level of a system or an organization after a security incident or violation has occurred. A physical intrusion is an unauthorized or unwanted entry

into a physical facility or area that contains sensitive or valuable assets, such as IT equipment, data, or personnel. A physical intrusion can cause damage, theft, sabotage, or espionage to the assets, and compromise the confidentiality, integrity, or availability of the information or services provided by the organization. A rapid response by guards or police to apprehend a possible intruder can prevent or limit the extent of the damage or loss caused by the physical intrusion, and deter or punish the intruder. A rapid response can also provide evidence or information for further investigation or prosecution of the incident.

NEW QUESTION: 786
某□□的□□管理□□□算得出，某□特定□□的□□价□(AV) □ 500,000 美元，□□敞口系数(EF) □ 20%。□□□的□次□失□期□ (SLE) 是多少？
A. 50,000美元
B. 10万美元
C. 250,000美元
D. 40万美元
Answer: B (LEAVE A REPLY)
SLE = AV ?EF = $500,000 ?0.20 = $100,000. SLE represents the monetary loss expected from a single occurrence of a risk event, and it is subsequently multiplied by the Annualized Rate of Occurrence (ARO) to calculate the Annualized Loss Expectancy (ALE).

NEW QUESTION: 787
在災難復原（DR）模擬過程中，發現共享復原站點缺乏足□的資料復原能力來支援多個計畫同時實施如果保持不變，這一事實會影響什麼？
A. 復原點目標 (RPO)
B. 復原時間目標 (RTO)
C. 業務影響分析 (BIA)
D. 投資報酬率 (ROI)
Answer: B (LEAVE A REPLY)
Disaster Recovery (DR) is the process of restoring the normal operations of an organization after a disaster, such as a fire, flood, earthquake, or cyberattack. DR planning involves identifying the critical business functions and processes, assessing the potential impacts and risks of a disaster, and developing strategies and procedures to recover from a disaster. One of the key metrics in DR planning is the Recovery Time Objective (RTO), which is the maximum acceptable time that a business function or process can be unavailable or disrupted after a disaster. RTO is determined by the business impact analysis (BIA), which evaluates the financial, operational, and reputational consequences of a prolonged downtime. RTO helps to prioritize the recovery of the most critical business functions and processes, and to allocate the necessary resources and personnel for the recovery. If the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously, the RTO of the affected business functions and processes would be impacted, as they would take longer to resume their normal operations.

NEW QUESTION: 788
為了讓安全漏洞的受害者在過失索賠中獲勝，受害者必須證明什麼？
A. 近因
B. 困難
C. 關注
D. 違反合約
Answer: A (LEAVE A REPLY)

NEW QUESTION: 789
作為設計原則，下列哪一位參與者負責識別和批准雲端生態系統中的資料安全要求？
A. 雲代理
B. 雲端提供者
C. 雲端消費者
D. 雲端審核員
Answer: C (LEAVE A REPLY)
As a design principle, the cloud consumer is the actor that is responsible for identifying and approving data security requirements in a cloud ecosystem. A cloud ecosystem is a complex system of interrelated and interdependent components that provide cloud services and solutions to the users and customers. A cloud ecosystem consists of different actors, such as cloud provider, cloud consumer, cloud broker, or cloud auditor, that have different roles and responsibilities in the cloud ecosystem. The cloud consumer is the actor that uses the cloud services or solutions provided by the cloud provider or the cloud broker. The cloud consumer is responsible for identifying and approving data security requirements in a cloud ecosystem, because:
The cloud consumer owns and controls the data that is stored, processed, or transmitted in the cloud ecosystem, and therefore, the cloud consumer has the authority and accountability for the data security requirements.
The cloud consumer knows and understands the data classification, sensitivity, and value of the data that is stored, processed, or transmitted in the cloud ecosystem, and therefore, the cloud consumer can determine the appropriate data security requirements.
The cloud consumer has the obligation and liability to comply with the data security regulations, standards, and best practices that apply to the data that is stored, processed, or transmitted in the cloud ecosystem, and therefore, the cloud consumer can define the relevant data security requirements.

NEW QUESTION: 790
以下哪□最能描述“网□分割”的目的？
A. 增加网□上可用的□□□
B. 将网□划分□更小、更独立的网段，以限制攻□范□并控制流量。
C. □所有□□分配静□IP地址
D. 消除□防火□的需求
Answer: B (LEAVE A REPLY)

Network segmentation divides a larger network into smaller subnetworks or zones, often separated by firewalls or VLANs, limiting lateral movement of an attacker and containing the potential impact of a security incident, while allowing more granular traffic control.

NEW QUESTION: 791
為了確保在整個生命週期中對資訊進行適當的治理，應先分配下列哪一項？
A. 所有者
B. 分類
C. 託管人
D. 保留
Answer: B (LEAVE A REPLY)
The data owner sometimes refer to as the organizational owner or senior manager is the person who has the ultimate organizational responsibility for data, the owner is typically the chief executive officer (CEO), president or a department head (DH). Data owners identify the classification of data and ensure that it is labeled properly.. in that case the first thing to assign is classification. my point is you dont assign the organizational owner.

NEW QUESTION: 792
下列哪一項是企業採用雲端技術的最大障礙？
A. 遷移週期
B. 資料完整性
C. 成本
D. 安全
Answer: D (LEAVE A REPLY)
While other factors like cost, migration period, and data integrity are important considerations, security tends to be the primary concern for many organizations when it comes to moving to the cloud. Companies often worry about:
Data privacy and protection in a cloud environment, especially when sensitive or regulated data is involved.
Control over data since the cloud service provider is responsible for maintaining the infrastructure, which might create concerns about unauthorized access, breaches, and compliance with regulations (such as GDPR, HIPAA, etc.).
Potential for data loss or downtime in case of cloud service disruptions.
Misconfigurations or human errors that can leave cloud environments vulnerable to attack.
Because security issues directly affect the confidentiality, integrity, and availability of data, they are often viewed as the greatest risk when transitioning to the cloud.

NEW QUESTION: 793
確保雲端服務供應商不會存取其基礎設施中儲存的客口資料的最有效方法是什麼？
A. 使用組織的加密工具和資料管理控制。
B. 確保雲端服務提供者依照合約規定不會存取數據，除非獲得明確的授權

C. 定期請求審核日誌。
D. 利用雲端提供者的金鑰管理和彈性硬體安全模組 (HSM) 支援。
Answer: A (LEAVE A REPLY)
Most secure is to avoid the use and reliance of CSP's key infrastructure and only use internal one.

NEW QUESTION: 794
以下哪□最能描述使用 VPN □行□程□公□“出口流量加密”的目的？
A. 加快□程□工的上网速度
B. □建一个安全加密的隧道，保□数据在□程□公人□的□□和企□网□之□通□不受信任的网□□□□的机密性和完整性。
C. 消除□多因素身份□□的需求
D. 自□修□□程□□
Answer: (SHOW ANSWER)
A VPN creates an encrypted tunnel between a remote worker's device and the corporate network, protecting the confidentiality and integrity of data in transit across untrusted networks (such as public Wi-Fi or the internet), and can also provide authentication and access control for remote connections.

NEW QUESTION: 795
下列哪一項提供了執行某項工作職能所需的最低權限集，並將使用者限制在具有所需權限的網域中？
A. 基於規則的訪問
B. 基於使用者角色的存取權限
C. 存取權限由系統決定
D. 基於數據敏感性的訪問
Answer: B (LEAVE A REPLY)
Access based on user's role provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges. This is also known as role- based access control (RBAC), which is a method of enforcing the principle of least privilege.
RBAC assigns permissions to roles rather than individual users, and users are assigned roles based on their responsibilities and qualifications

NEW QUESTION: 796
未安裝電湧保護器時的補償控制是什麼？
A. 與網站□建的網路服務供應商建立雙線
B. 現場安裝備用柴油發電機
C. 站點具有熱災難復原 (DR) 環境
D. 站點□有雙活集群中的網路設備
Answer: (SHOW ANSWER)
A compensating control is a measure that is taken to reduce the risk of an existing or potential control weakness. Electrical surge protectors are devices that protect electrical equipment from voltage spikes caused by lightning, power outages, or other disturbances. If surge protectors are not installed, the risk

of damage to network equipment and data loss is increased. A backup diesel generator is a compensating control that can provide uninterrupted power supply to the network equipment in case of a power failure, thus reducing the impact of electrical surges.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

NEW QUESTION: 797
安全營運中心 (SOC) 在伺服器上收到事件回應通知，其中存在已植入後門的活躍入侵者。發送初始通知並建立通訊。
在執行下一步之前必須考慮或評估什麼？
A. 在對伺服器硬碟的內容進行雜湊處理之前通知執法部門至關重要
B. 確定事件的執行者比事件如何發生更重要
C. 從網路中刪除伺服器可能會阻止捕獲入侵者
D. 將硬碟的內容複製到另一個儲存裝置可能會損壞證據
Answer: C (LEAVE A REPLY)
Before performing the next step in an incident response, it must be considered or evaluated that removing the server from the network may prevent catching the intruder who has planted a backdoor. This is because the intruder may still be connected to the server or may try to reconnect later, and disconnecting the server may alert the intruder or lose the opportunity to trace the intruder's source or identity. Therefore, it may be better to isolate the server from the network or monitor the network traffic to gather more evidence and information about the intruder.
Notifying law enforcement, identifying who executed the incident, and copying the contents of the hard drive are not the factors that must be considered or evaluated before performing the next step, as they are either irrelevant or premature at this stage of the incident response.

NEW QUESTION: 798
業務連續性計劃 (BCP) 何時被視為有效？
A. 當業務連續性 (BC) 經理驗證後
B. 經董事會確認後
C. 當它已被所有威脅場景驗證時
D. 經過實際練習驗證後
Answer: D (LEAVE A REPLY)
A Business Continuity Plan (BCP) is considered to be valid when it has been validated by realistic exercises. A BCP is a part of a BCP/DRP that focuses on ensuring the continuous operation of the

organization's critical business functions and processes during and after a disruption or disaster. A BCP should include various components, such as:
Business impact analysis: a process that identifies and prioritizes the critical business functions and processes, and assesses the potential impacts and risks of a disruption or disaster on them Recovery strategies: a process that defines and selects the appropriate methods and resources to recover the critical business functions and processes, such as alternate sites, backup systems, or recovery teams BCP document: a document that outlines and details the scope, purpose, and features of the BCP, such as the roles and responsibilities, the recovery procedures, and the contact information Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the BCP, and educates and trains the relevant stakeholders, such as the staff, the management, and the customers, on the BCP and their roles and responsibilities Maintenance and review: a process that monitors and updates the BCP, and addresses any changes or issues that might affect the BCP, such as the business requirements, the threat landscape, or the feedback and lessons learned A BCP is considered to be valid when it has been validated by realistic exercises, because it can ensure that the BCP is practical and applicable, and that it can achieve the desired outcomes and objectives in a real-life scenario. Realistic exercises are a type of testing, training, and exercises that involve performing and practicing the BCP with the relevant stakeholders, using simulated or hypothetical scenarios, such as a fire drill, a power outage, or a cyberattack. Realistic exercises can provide several benefits, such as:
Improving the confidence and competence of the organization and its staff in handling a disruption or disaster Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks

NEW QUESTION: 799
安全軟體開發生命週期 (SDLC) 期望應用程式程式碼以一致的方式編寫，以便於審核，下列哪一項？
A. 保護
B. 正在執行
C. 複製
D. 增強
Answer: D (LEAVE A REPLY)
The Security Software Development Life Cycle (SDLC) is a framework that guides the development of secure software applications. It integrates security principles and practices throughout the entire software development process, from planning and analysis to design, implementation, testing, deployment, and maintenance. One of the expectations of the Security SDLC is that the application code should be written in a consistent manner to allow ease of auditing and enhancing. Auditing is the process of reviewing and verifying the code for compliance, quality, and security. Enhancing is the process of improving and modifying the code to meet changing requirements, fix bugs, or add new features. Writing code in a consistent manner helps to facilitate auditing and enhancing by making the code more readable, understandable, and maintainable.

NEW QUESTION: 800
連接兩個園區網路的光纖鏈路中斷。工程師應該使用下列哪一種工具來偵測光纖鏈路的確切斷點？
A. OTDR
B. 音調口生器
C. 熔接機
D. 電纜測試儀
E. PoE 注入器
Answer: A (LEAVE A REPLY)
An OTDR (optical time domain reflectometer) is a tool that can be used to detect the exact break point of a fiber link. An OTDR works by sending a pulse of light into the fiber and measuring the time and intensity of the reflected light that comes back. By analyzing the reflected light, the OTDR can determine the distance, location, and severity of any faults or breaks in the fiber link.
An OTDR can also provide information about the attenuation, splice loss, and connector loss of the fiber link.

NEW QUESTION: 801
下列哪一種存取控制機制使用一組編碼的安全相關屬性來表徵主體和客體？
A. 強制存取控制 (MAC)
B. 基於角色的存取控制 (RBAC)
C. 基於屬性的存取控制 (ABAC)
D. 自主存取控制 (DAC)
Answer: C (LEAVE A REPLY)
Attribute-based access control (ABAC) is an access control mechanism that characterizes subjects (users, processes) and objects (resources) using a set of encoded security-relevant attributes or properties. ABAC allows for fine-grained access control decisions based on various attributes such as user roles, resource classifications, time of access, and other contextual information. This flexibility in defining access policies makes ABAC suitable for complex and dynamic access control scenarios.

NEW QUESTION: 802
電腦取證需要下列哪些主要步驟？
A. 向相關部門通報事件，分析數據，並整理數據以進行關聯分析
B. 採取措施控制損失，向相關部門通報事件，並分析數據
C. 取得數據而不進行任何更改，驗證恢復的數據，並分析數據
D. 在數據銷毀前取得數據，整合數據進行關聯分析，並採取措施控制損失
Answer: C (LEAVE A REPLY)
The main steps that computer forensics requires are to acquire the data without altering, authenticate the recovered data, and analyze the data. Computer forensics is the process of collecting, preserving, and examining digital evidence from computers or other electronic devices, such as smartphones,

tablets, or cameras. Computer forensics follows a standard methodology that consists of the following steps:

Acquire the data without altering: This step involves creating a bit-by-bit copy or image of the original data source, such as a hard disk, a memory card, or a network packet, without modifying or damaging the original data. This ensures the integrity and the admissibility of the digital evidence in a court of law.

Authenticate the recovered data: This step involves verifying that the copied or imaged data is identical to the original data, and that it has not been tampered with or corrupted during the acquisition process. This can be done by using cryptographic hash functions, such as MD5 or SHA-1, that generate a unique and fixed-length value for the data, and comparing the hash values of the original and the copied data.

Analyze the data: This step involves examining the data for any relevant information or clues that can help to answer the questions or solve the problems related to the investigation. This can involve various techniques, such as keyword searching, file carving, timeline analysis, or malware analysis, depending on the type and the purpose of the data.

Valid CISSP-CN Dumps shared by Actual4test.com for Helping Passing CISSP-CN Exam! Actual4test.com now offer the **newest CISSP-CN exam dumps**, the Actual4test.com CISSP-CN exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CISSP-CN dumps with Test Engine here: https://www.actual4test.com/CISSP-CN_examcollection.html (**1811** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)