CompTIA.SY0-701.v2025-07-14.q247

Exam Code:	SY0-701
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	247
Version:	v2025-07-14
# of views:	106
# of Questions views:	2470
https://www.freepdfdumps.com/CompTIA.SY0-701.v2025-07-14.q247.html	

NEW QUESTION: 1
An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?
A. XDR
B. SPF
C. DLP
D. DMARC
Answer: C (LEAVE A REPLY)
To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.
XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.
SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.
DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

NEW QUESTION: 2
Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?
A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation
Answer: A (LEAVE A REPLY)

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones. Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

NEW QUESTION: 3
A company implemented an MDM policy 10 mitigate risks after repealed instances of employees losing company-provided mobile phones. In several cases. The lost phones were used maliciously to perform social engineering attacks against other employees. Which of the following MDM features should be configured to best address this issue? (Select two).
A. Screen locks
B. Remote wipe
C. Full device encryption
D. Push notifications
E. Application management
F. Geolocation
Answer: A,B (LEAVE A REPLY)
Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.
References =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

NEW QUESTION: 4
Which of the following is a primary security concern for a company setting up a BYOD program?
A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking
Answer: D (LEAVE A REPLY)
Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's

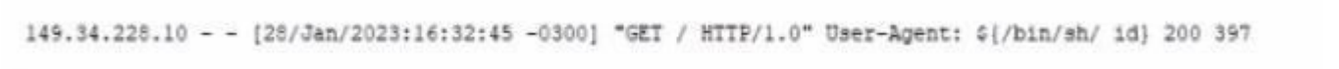
restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page
76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

NEW QUESTION: 5
Which of the following is the most likely to be included as an element of communication in a security awareness program?
A. Reporting phishing attempts or other suspicious activities
B. Detecting insider threats using anomalous behavior recognition
C. Verifying information when modifying wire transfer data
D. Performing social engineering as part of third-party penetration testing
Answer: A (LEAVE A REPLY)
A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.
The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information

related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training - CompTIA Security+ SY0-701: 5.2, video at 0: 00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

NEW QUESTION: 6
Which of the following should be used to aggregate log data in order to create alerts and detect anomalous activity?
A. SIEM
B. WAF
C. Network taps
D. IDS
Answer: A (LEAVE A REPLY)
A Security Information and Event Management (SIEM) solution collects, aggregates, and correlates logs from multiple sources to detect anomalies and generate alerts. SIEMs are essential for security monitoring and incident detection.References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 7
A security analyst is reviewing logs and discovers the following:



Which of the following should be used lo best mitigate this type of attack?
A. Secure cookies
B. Input sanitization
C. Static code analysis
D. Sandboxing
Answer: (SHOW ANSWER)

NEW QUESTION: 8
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?
A. ACL
B. DLP

C. IDS
D. IPS
Answer: D (LEAVE A REPLY)
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION: 9
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?
A. Real-time recovery
B. Hot
C. Cold
D. Warm
Answer: C (LEAVE A REPLY)
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. References = CompTIA Security+ SY0-701 Certification Study Guide, page 387; Backup Types - SY0-601 CompTIA Security+ : 2.5, video at 4:50.

NEW QUESTION: 10
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?
A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor
Answer: B (LEAVE A REPLY)
= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is

isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances - SY0-601 CompTIA Security+ :
3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

NEW QUESTION: 11
An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?
A. Network
B. System
C. Application
D. Authentication
Answer: A (LEAVE A REPLY)
To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.
References =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

NEW QUESTION: 12
A systems administrator is working on a solution with the following requirements:
* Provide a secure zone.
* Enforce a company-wide access control policy.
* Reduce the scope of threats.
Which of the following is the systems administrator setting up?
A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA
Answer: (SHOW ANSWER)
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide

a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company- wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

NEW QUESTION: 13
A legal department must maintain a backup from all devices that have been shredded and recycled by a third party. Which of the following best describes this requirement?
A. Destruction
B. Sanitation
C. Data retention
D. Certification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?
A. Jump server
B. RADIUS
C. HSM
D. Load balancer
Answer: (SHOW ANSWER)
A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host12.
RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access34.
HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them5 .
A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them . References = How to access

a remote server using a jump host Jump server RADIUS Remote Authentication Dial-In User Service (RADIUS) Hardware Security Module (HSM)
[What is an HSM?]
[Load balancing (computing)]
[What is Load Balancing?]

NEW QUESTION: 15
A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?
A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement
Answer: A (LEAVE A REPLY)
End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget. References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 29 1

NEW QUESTION: 16
A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network.
Which of the following should be configured on the existing network infrastructure to best prevent this activity?
A. Port security
B. Virtual private network
C. Transport layer security
D. Web application firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following allows an exploit to go undetected by the operating system?
A. Firmware vulnerabilities
B. Encrypted payloads
C. Side loading
D. Memory injection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following examples would be best mitigated by input sanitization?
A. <script>alert ("Warning!") ,-</script>
B. nmap - 10.11.1.130
C. Email message: "Click this link to get your free gift card."
D. Browser message: "Your connection is not private."
Answer: A (LEAVE A REPLY)
This example of a script injection attack would be best mitigated by input sanitization. Input sanitization involves cleaning or filtering user inputs to ensure that they do not contain harmful data, such as malicious scripts. This prevents attackers from executing script-based attacks (e.g., Cross-Site Scripting or XSS).
Nmap command is unrelated to input sanitization, as it is a network scanning tool.
Email phishing attempts require different mitigations, such as user training.
Browser warnings about insecure connections involve encryption protocols, not input validation

NEW QUESTION: 19
A security manager created new documentation to use in response to various types of security incidents.
Which of the following is the next step the manager should take?
A. Set the maximum data retention policy.
B. Securely store the documents on an air-gapped network.
C. Review the documents' data classification policy.
D. Conduct a tabletop exercise with the team.
Answer: D (LEAVE A REPLY)
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents.

NEW QUESTION: 20
Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?
A. Automation
B. Compliance checklist
C. Attestation
D. Manual audit
Answer: A (LEAVE A REPLY)
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort.
Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs.
Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.
The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:
Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.
Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.
Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. :
CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION: 21
Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.

Which of the following changes would allow users to access the site?
A. Creating a firewall rule to allow HTTPS traffic
B. Configuring the IPS to allow shopping
C. Tuning the DLP rule that detects credit card data
D. Updating the categorization in the content filter
Answer: (SHOW ANSWER)
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.

NEW QUESTION: 22
A systems administrator receives the following alert from a file integrity monitoring tool:
The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months.
Which of the following most likely occurred?
A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.
Answer: D (LEAVE A REPLY)
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page
147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

NEW QUESTION: 23
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?
A. Scalability
B. Availability
C. Cost

D. Ease of deployment

Answer: B (LEAVE A REPLY)

Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial- of-service attacks, and have backup and recovery plans in case of failures2.

NEW QUESTION: 24

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

A. White

B. Purple

C. Blue

D. Red

Answer: (SHOW ANSWER)

A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams - SY0-601 CompTIA Security+ : 1.8

NEW QUESTION: 25

Which of the following elements of digital forensics should a company use If It needs to ensure the integrity of evidence?

A. Containment

B. Acquisition

C. Preservation

D. E-discovery

Answer: C (LEAVE A REPLY)

NEW QUESTION: 26

A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following is the best method to achieve this objective?

A. Vulnerability scans
B. Penetration testing
C. Internal auditing
D. Third-party attestation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
During a recent log review, an analyst found evidence of successful injection attacks. Which of the following will best address this issue?
A. Authentication
B. Secure cookies
C. Static code analysis
D. Input validation
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Input validation ensures that only properly formatted and expected input is accepted by an application, preventing injection attacks such as SQL injection and command injection. Properly validating and sanitizing user inputs can mitigate these types of attacks.
* Authentication (A) helps verify user identity but does not prevent injection attacks.
* Secure cookies (B) protect session data but do not stop injection-based exploits.
* Static code analysis (C) can help identify vulnerabilities but does not actively prevent injection attacks in real-time.
Implementing strong input validation can prevent malicious code from being executed, reducing the risk of injection attacks.

NEW QUESTION: 28
Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?
A. Mitigate
B. Accept
C. Transfer
D. Avoid
Answer: A (LEAVE A REPLY)
Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the

consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process. These strategies may not be feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation2

NEW QUESTION: 29
Which of the following should a security operations center use to improve its incident response procedure?
A. Playbooks
B. Frameworks
C. Baselines
D. Benchmarks
Answer: A (LEAVE A REPLY)
A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation.
Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.
Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.
Benchmarks are performance standards and are not directly related to incident response.

NEW QUESTION: 30
A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected. Most employees clocked in and out while they were Inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while Inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.
Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet. Which of the following Is the most likely reason for this compromise?
A. A brute-force attack was used against the time-keeping website to scan for common passwords.

B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.
C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site
D. ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.machine.
Answer: (SHOW ANSWER)
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.
References =
CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

NEW QUESTION: 31
A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?
A. Deploying PowerShell scripts
B. Pushing GPO update
C. Enabling PAP
D. Updating EDR profiles
Answer: (SHOW ANSWER)
A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

NEW QUESTION: 32
A customer of a large company receives a phone call from someone claiming to work for the company and asking for the customer's credit card information. The customer sees the caller ID is the same as the company's main phone number. Which of the following attacks is the customer most likely a target of?
A. Vishing
B. Smishing
C. Phishing
D. Whaling
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?
A. IDS
B. ACL
C. EDR
D. NAC
Answer: C (LEAVE A REPLY)
Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

NEW QUESTION: 34
A company is discarding a classified storage array and hires an outside vendor to complete the disposal.
Which of the following should the company request from the vendor?
A. Certification
B. Inventory list
C. Classification
D. Proof of ownership

Answer: A (LEAVE A REPLY)
The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

NEW QUESTION: 35
A user would like to install software and features that are not available with a smartphone's default software.
Which of the following would allow the user to install unauthorized software and enable new features?
A. SOU
B. Cross-site scripting
C. Jailbreaking
D. Side loading
Answer: C (LEAVE A REPLY)
Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.
SOU (Statement of Understanding) is not related to modifying devices.
Cross-site scripting is a web-based attack technique, unrelated to smartphone software.
Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

NEW QUESTION: 36
Which of the following is a reason environmental variables are a concern when reviewing potential system vulnerabilities?
A. The contents of environmental variables could affect the scope and impact of an exploited vulnerability.
B. In-memory environmental variable values can be overwritten and used by attackers to insert malicious code.
C. Environmental variables define cryptographic standards for the system and could create vulnerabilities if deprecated algorithms are used.
D. Environmental variables will determine when updates are run and could mitigate the likelihood of vulnerability exploitation.
Answer: (SHOW ANSWER)

Environmental variables store configuration settings, paths, and other system-related information that applications and processes use. If an attacker gains access to these variables, they could manipulate them to alter application behavior, gain unauthorized access, or escalate privileges. For example, an attacker could modify the PATH variable to execute malicious programs instead of legitimate ones. This can significantly increase the scope and impact of an exploited vulnerability, making it a major security concern.

NEW QUESTION: 37
A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?
A. Implementing a bastion host
B. Deploying a perimeter network
C. Installing a WAF
D. Utilizing single sign-on
Answer: A (LEAVE A REPLY)
A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes12.
A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise3.
Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public- facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security4.
Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats5.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign- on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached6. References = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

NEW QUESTION: 38
A network administrator wants to ensure that network traffic is highly secure while in transit.
Which of the following actions best describes the actions the network administrator should take?
A. Ensure the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.
B. Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.
C. Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.
D. Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
A company is developing a critical system for the government and storing project information on a fileshare.
Which of the following describes how this data will most likely be classified? (Select two).
A. Private
B. Confidential
C. Public
D. Operational
E. Urgent
F. Restricted
Answer: B,F (LEAVE A REPLY)
Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:
Public: Data that can be freely disclosed to anyone without any harm or risk.
Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.
Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.
In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2.
References: 1: CompTIA Security+ Study Guide: Exam SY0-701,
9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

NEW QUESTION: 40
A growing organization, which hosts an externally accessible application, adds multiple virtual servers to improve application performance and decrease the resource usage on individual servers Which of the following solutions is the organization most likely to employ to further increase performance and availability?
A. Jump server
B. SD-WAN
C. Proxy server
D. Load balancer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
A security engineer configured a remote access VPN. The remote access VPN allows end users to connect to the network by using an agent that is installed on the endpoint, which establishes an encrypted tunnel. Which of the following protocols did the engineer most likely implement?
A. IPSec
B. GRE
C. EAP
D. SD-WAN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following would be the best way to handle a critical business application that is running on a legacy server?
A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning
Answer: C (LEAVE A REPLY)

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.
One of the best ways to handle a legacy server running a critical business application is to harden it.
Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:
Applying patches and updates to the operating system and the application, if available Removing or disabling unnecessary services, features, or accounts Configuring firewall rules and network access control lists to restrict inbound and outbound traffic Enabling encryption and authentication for data transmission and storage Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.

NEW QUESTION: 43
Which of the following would most likely be used by attackers to perform credential harvesting?
A. Supply chain compromise
B. Rainbow table
C. Third-party software
D. Social engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 44
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?
A. Clustering servers
B. Geographic dispersion
C. Load balancers
D. Off-site backups
Answer: (SHOW ANSWER)
Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network. Geographic dispersion can also enhance

the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption12.
The other options are not the best ways to address the company's concern:
Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system. Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building3.
Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources. Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building4.
Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

NEW QUESTION: 45
Which of the following would enable a data center to remain operational through a multiday power outage?
A. Uninterruptible power supply
B. Replication
C. Parallel processing
D. Generator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following documents details how to accomplish a technical security task?
A. Standard
B. Policy
C. Guideline
D. Procedure
Answer: D (LEAVE A REPLY)
A procedure provides step-by-step instructions on how to complete a specific security task, ensuring consistency and accuracy. Unlike policies, which define high-level security expectations, procedures are detailed and operational. For example, a password reset procedure would outline the exact steps IT support must follow when assisting users.

* Policy: Defines security objectives and rules (e.g., "All passwords must be complex").
* Standard: Specifies required technologies or configurations.
* Guideline: Provides recommendations but is not mandatory.
* Procedure: Gives exact instructions to perform tasks.

NEW QUESTION: 47
A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?
A. Appetite
B. Register
C. Threshold
D. Tolerance
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).
A. The device has been moved from a production environment to a test environment.
B. The device is configured to use cleartext passwords.
C. The device is moved to an isolated segment on the enterprise network.
D. The device is moved to a different location in the enterprise.
E. The device's encryption level cannot meet organizational standards.
F. The device is unable to receive authorized updates.
Answer: E (LEAVE A REPLY)
An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.
References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671
CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

NEW QUESTION: 49
An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?
A. Cloud-based
B. Peer-to-peer
C. On-premises
D. Hybrid
Answer: A (LEAVE A REPLY)
Cloud-based models provide strong security with features like encryption, redundancy, and disaster recovery, making it a secure choice for international operations.

NEW QUESTION: 50
Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?
A. Automated scanning
B. Penetration testing
C. Threat hunting
D. Log aggregation
E. Adversarial emulation
Answer: A (LEAVE A REPLY)
Automated vulnerability scanning is the first step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.
* Penetration testing (B) is conducted after vulnerabilities are identified.
* Threat hunting (C) focuses on detecting unknown threats, not listing vulnerabilities.

NEW QUESTION: 51
Which of the following is a hardware-specific vulnerability?
A. Firmware version
B. Buffer overflow
C. SQL injection
D. Cross-site scripting
Answer: A (LEAVE A REPLY)
Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific

vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity. References = CompTIA Security + Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 67. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1, page
10.

NEW QUESTION: 52
A company wants to track modifications to the code used to build new virtual servers. Which of the following will the company most likely deploy?
A. Change management ticketing system
B. Behavioral analyzer
C. Collaboration platform
D. Version control tool
Answer: D (LEAVE A REPLY)
Detailed Explanation:A version control tool, such as Git, tracks changes made to code, maintains history, and allows developers to manage and revert to earlier versions when needed. This ensures accountability and control over modifications. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Version Control and Documentation".

NEW QUESTION: 53
Sine a recent upgrade (o a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings. Which of the following installation considerations should the security team evaluate next?
A. Channel overlap
B. Encryption type
C. New WLAN deployment
D. WAP placement
Answer: A (LEAVE A REPLY)
When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.
References = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

NEW QUESTION: 54

An attacker used XSS to compromise a web server. Which of the following solutions could have been used to prevent this attack?

A. NGFW

B. UTM

C. WAF

D. NAC

Answer: C (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:

A Web Application Firewall (WAF) is designed to protect web applications from attacks such as Cross- Site Scripting (XSS) by filtering and monitoring HTTP traffic between the internet and a web application.

* Next-Generation Firewalls (NGFW) (A) provide advanced network security but are not specifically designed to protect web applications from XSS attacks.
* Unified Threat Management (UTM) (B) provides multiple security functions but lacks the specialized application-layer protection needed to mitigate XSS.
* Network Access Control (NAC) (D) controls device access to the network but does not prevent web- based attacks.

A WAF is the best solution for protecting web servers from XSS, SQL injection, and other web-based threats.

NEW QUESTION: 55

A systems administrator is auditing all company servers to ensure. They meet the minimum security baseline While auditing a Linux server, the systems administrator observes the /etc/shadow file has permissions beyond the baseline recommendation. Which of the following commands should the systems administrator use to resolve this issue?

A. chmod

B. grep

C. dd

D. passwd

Answer: A (LEAVE A REPLY)

The chmod command is used to change file permissions on Unix and Linux systems. If the /etc/shadow file has permissions beyond the baseline recommendation, the systems administrator should use chmod to modify the file's permissions, ensuring it adheres to the security baseline and limits access to authorized users only.

References = CompTIA Security+ SY0-701 study materials, focusing on system hardening and file permissions management.

NEW QUESTION: 56

An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas.

The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this stream is encrypted and authenticated. Which of the following protocols should be implemented to best meet this objective?

A. SSH

B. SRTP

C. S/MIME

D. PPTP

Answer: B (LEAVE A REPLY)

Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.

NEW QUESTION: 57

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

A. Serverless architecture

B. Thin clients

C. Private cloud

D. Virtual machines

Answer: (SHOW ANSWER)

Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance.

Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.

References =

CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

NEW QUESTION: 58

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software

C. Performing static code analysis on the software

D. Ensuring secure cookies are use

Answer: B (LEAVE A REPLY)

Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

NEW QUESTION: 59
An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?
A. Malicious flash drive
B. Remote access Trojan
C. Brute-forced password
D. Cryptojacking
Answer: D (LEAVE A REPLY)
Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.
References =
CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

NEW QUESTION: 60
Which of the following topics would most likely be included within an organization's SDLC?
A. Service-level agreements
B. Information security policy
C. Penetration testing methodology
D. Branch protection requirements
Answer: B (LEAVE A REPLY)
Within an organization's Software Development Life Cycle (SDLC), an Information Security Policy is a vital component. It outlines the rules and procedures for ensuring that the organization's IT assets and data are protected throughout the development process. Ensuring secure coding

practices, access controls, and regular security testing is fundamental in preventing vulnerabilities in applications.
Other options like service-level agreements and branch protection requirements are less likely to be integral to SDLC processes. Penetration testing methodology, while useful, is generally considered outside the scope of the SDLC.

NEW QUESTION: 61
Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?
A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist
Answer: C (LEAVE A REPLY)
A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare12. References = 1:
CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors - CompTIA Security+ SY0-701 - 2.1, video by Professor Messer.

NEW QUESTION: 62
A security administrator recently reset local passwords and the following values were recorded in the system:

Host	Account	MD5 password values
ACCT-PC-1	admin	f1bdf5ed1d7ad7ede4e3809bd35644b0
HR-PC-1	admin	d706ab8258fe67c131ebc57a6e29184
IT-PC-2	admin	f8ddb9ebb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following in the security administrator most likely protecting against?
A. Account sharing
B. Weak password complexity

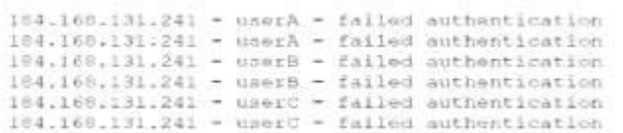
C. Pass-the-hash attacks
D. Password compromise
Answer: (SHOW ANSWER)
The scenario shows MD5 hashed password values. The most likely reason the security administrator is focusing on these values is to protect against pass-the-hash attacks. In this type of attack, an attacker can use a captured hash to authenticate without needing to know the actual plaintext password. By managing and monitoring these hashes, the administrator can implement strategies to mitigate this type of threat.
References =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

NEW QUESTION: 63
A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)
A. If a security incident occurs on the device, the correct employee can be notified.
B. The security team will be able to send user awareness training to the appropriate device.
C. Users can be mapped to their devices when configuring software MFA tokens.
D. User-based firewall policies can be correctly targeted to the appropriate laptops.
E. When conducting penetration testing, the security team will be able to target the desired laptops.
F. Company data can be accounted for when the employee leaves the organization.
Answer: (SHOW ANSWER)
Labeling all laptops with asset inventory stickers and associating them with employee IDs can provide several security benefits for a company. Two of these benefits are:
A: If a security incident occurs on the device, the correct employee can be notified. An asset inventory sticker is a label that contains a unique identifier for a laptop, such as a serial number, a barcode, or a QR code. By associating this identifier with an employee ID, the security team can easily track and locate the owner of the laptop in case of a security incident, such as a malware infection, a data breach, or a theft. This way, the security team can notify the correct employee about the incident, and provide them with the necessary instructions or actions to take, such as changing passwords, scanning for viruses, or reporting the loss. This can help to contain the incident, minimize the damage, and prevent further escalation.
F: Company data can be accounted for when the employee leaves the organization. When an employee leaves the organization, the company needs to ensure that all the company data and assets are returned or deleted from the employee's laptop. By labeling the laptop with an asset inventory sticker and associating it with an employee ID, the company can easily identify and verify the laptop that belongs to the departing employee, and perform the appropriate data backup, wipe, or transfer procedures. This can help to protect the company data from unauthorized access, disclosure, or misuse by the former employee or any other party.

The other options are not correct because they are not related to the security benefits of labeling laptops with asset inventory stickers and associating them with employee IDs. B. The security team will be able to send user awareness training to the appropriate device. User awareness training is a type of security education that aims to improve the knowledge and behavior of users regarding security threats and best practices. The security team can send user awareness training to the appropriate device by using the email address, username, or IP address of the device, not the asset inventory sticker or the employee ID. C. Users can be mapped to their devices when configuring software MFA tokens. Software MFA tokens are a type of multi- factor authentication that uses a software application to generate a one-time password or a push notification for verifying the identity of a user. Users can be mapped to their devices when configuring software MFA tokens by using the device ID, phone number, or email address of the device, not the asset inventory sticker or the employee ID. D. User-based firewall policies can be correctly targeted to the appropriate laptops. User- based firewall policies are a type of firewall rules that apply to specific users or groups of users, regardless of the device or location they use to access the network. User-based firewall policies can be correctly targeted to the appropriate laptops by using the username, domain, or certificate of the user, not the asset inventory sticker or the employee ID. E. When conducting penetration testing, the security team will be able to target the desired laptops. Penetration testing is a type of security assessment that simulates a real-world attack on a network or system to identify and exploit vulnerabilities. When conducting penetration testing, the security team will be able to target the desired laptops by using the IP address, hostname, or MAC address of the laptop, not the asset inventory sticker or the employee ID. References = CompTIA Security+ Study Guide (SY0-701), Chapter 1: General Security Concepts, page 17. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.4: Asset Management, video: Asset Inventory (6:12).

NEW QUESTION: 64

The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced faded log-In attempts when authenticating from the same IP address:



Which of the following most likely describes attack that took place?

A. Spraying

B. Brute-force

C. Dictionary

D. Rainbow table

Answer: A (LEAVE A REPLY)

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for

many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

NEW QUESTION: 65
Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?
A. Hacktivist
B. Whistleblower
C. Organized crime
D. Unskilled attacker
Answer: (SHOW ANSWER)
Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption12. References = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

NEW QUESTION: 66
After reviewing the following vulnerability scanning report:
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
A security analyst performs the following test:
nmap -p 23 192.168.14.6 -script telnet-encryption
PORT STATE SERVICE REASON
23/tcp open telnet syn-ack
I telnet encryption:
| _ Telnet server supports encryption
Which of the following would the security analyst conclude for this reported vulnerability?
A. It is a false positive.
B. A rescan is required.
C. It is considered noise.
D. Compensating controls exist.
Answer: A (LEAVE A REPLY)

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly3. References: 3: Telnet Protocol - Can You Encrypt Telnet?

NEW QUESTION: 67
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?
A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response
Answer: (SHOW ANSWER)
Detailed Explanation:
A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 5: Security Program Management, Section: "Incident Response Planning and Exercises".

NEW QUESTION: 68
A security analyst is creating base for the server team to follow when hardening new devices for deployment.
Which of the following beet describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide
Answer: D (LEAVE A REPLY)
The security analyst is creating a "secure configuration guide," which is a set of instructions or guidelines used to configure devices securely before deployment. This guide ensures that the devices are set up according to best practices to minimize vulnerabilities and protect against potential security threats.
References =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on System Hardening and Secure Configuration.

NEW QUESTION: 69
Which of the following can best protect against an employee inadvertently installing malware on a company system?
A. Host-based firewall
B. System isolation
C. Least privilege
D. Application allow list
Answer: D (LEAVE A REPLY)
An application allow list is a security technique that specifies which applications are authorized to run on a system and blocks all other applications. An application allow list can best protect against an employee inadvertently installing malware on a company system because it prevents the execution of any unauthorized or malicious software, such as viruses, worms, trojans, ransomware, or spyware. An application allow list can also reduce the attack surface and improve the performance of the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 551 1

NEW QUESTION: 70
A security architect wants to prevent employees from receiving malicious attachments by email. Which of the following functions should the chosen solution do?
A. Tap and monitor the email feed.
B. Check SPF records.
C. Scan email traffic inline.
D. Apply IP address reputation data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
A security professional discovers a folder containing an employee's personal information on the enterprise's shared drive. Which of the following best describes the data type the security professional should use to identify organizational policies and standards concerning the storage of employees' personal information?
A. Legal
B. Financial
C. Privacy
D. Intellectual property
Answer: C (LEAVE A REPLY)
Detailed Explanation:Privacy data includes information such as Personally Identifiable Information (PII), which relates to employees' or customers' personal data. Organizations often maintain policies and standards specifically addressing how such sensitive information should be handled.

Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Types and Classifications".

NEW QUESTION: 72
A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?
A. Installing HIDS on the system
B. Placing the system in an isolated VLAN
C. Decommissioning the system
D. Encrypting the system's hard drive
Answer: B (LEAVE A REPLY)
To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.
Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.
Decommissioning may not be feasible if the system is critical.
Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

NEW QUESTION: 73
A systems administrator needs to ensure the secure communication of sensitive data within the organization's private cloud. Which of the following is the best choice for the administrator to implement?
A. IPSec
B. SHA-1
C. RSA
D. TGT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
Which of the following cryptographic solutions protects data at rest?
A. Steganography
B. Full disk encryption
C. Digital signatures
D. Private key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.
Which of the following should the organization deploy to best protect against similar attacks in the future?
A. NGFW
B. WAF
C. TLS
D. SD-WAN
Answer: (SHOW ANSWER)
A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data. References = Buffer Overflows - CompTIA Security+ SY0-701 - 2.3, Web Application Firewalls - CompTIA Security+ SY0-701 - 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

NEW QUESTION: 76
Which of the following involves an attempt to take advantage of database misconfigurations?
A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection
Answer: B (LEAVE A REPLY)
SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

NEW QUESTION: 77
A security engineer at a large company needs to enhance IAM to ensure that employees can only access corporate systems during their shifts. Which of the following access controls should the security engineer implement?
A. Role-based
B. Time-of-day restrictions
C. Least privilege
D. Biometric authentication
Answer: (SHOW ANSWER)
Detailed Explanation:
Time-of-day restrictions limit access to corporate systems based on predefined schedules. This ensures employees can only access resources during their assigned work hours. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Models".

NEW QUESTION: 78
Which of the following is a type of vulnerability that involves inserting scripts into web-based applications in order to take control of the client's web browser?
A. SQL injection
B. Cross-site scripting
C. Zero-day exploit
D. On-path attack
Answer: B (LEAVE A REPLY)
Cross-site scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into a website, which are then executed in the user's web browser, potentially leading to data theft or session hijacking.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 79
An administrator must replace an expired SSL certificate. Which of the following does the administrator need to create the new SSL certificate?
A. CSR

B. OCSP
C. Key
D. CRL
Answer: A (LEAVE A REPLY)
A Certificate Signing Request (CSR) is a request sent to a certificate authority (CA) to issue an SSL certificate. The CSR contains information like the public key, which will be part of the certificate.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 80
A security analyst has determined that a security breach would have a financial impact of $15,000 and is expected to occur twice within a three-year period. Which of the following is the ALE for this risk?
A. $15,000
B. $7,500
C. $30,000
D. $10,000
Answer: (SHOW ANSWER)

NEW QUESTION: 81
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?
A. Multifactor authentication
B. Permissions assignment
C. Access management
D. Password complexity
Answer: A (LEAVE A REPLY)
The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user' s password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication.
Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References = You can learn more about multifactor authentication and other security concepts in the following resources:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1
Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2 Multi-factor Authentication - SY0-601 CompTIA Security+ : 2.43 TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4
CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

NEW QUESTION: 82
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: C (LEAVE A REPLY)
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

NEW QUESTION: 83
After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?
A. Compensating
B. Detective
C. Preventive
D. Corrective
Answer: (SHOW ANSWER)
Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that

occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.

NEW QUESTION: 84
Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?
A. To track the status of patching installations
B. To find shadow IT cloud deployments
C. To continuously the monitor hardware inventory
D. To hunt for active attackers in the network
Answer: (SHOW ANSWER)
Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.
Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.
Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

NEW QUESTION: 85
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?
A. Tuning
B. Aggregating
C. Quarantining
D. Archiving
Answer: A (LEAVE A REPLY)
Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations

center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope.
Therefore, this is the best answer among the given options. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

NEW QUESTION: 86
Which of the following is used to add extra complexity before using a one-way data transformation algorithm?
A. Key stretching
B. Data masking
C. Steganography
D. Salting
Answer: D (LEAVE A REPLY)
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks. References = Passwords technical overview Encryption, hashing, salting - what's the difference?
Salt (cryptography)

NEW QUESTION: 87
A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?
A. Application
B. IPS/IDS
C. Network
D. Endpoint
Answer: D (LEAVE A REPLY)
An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.

An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.
An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.
A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.
Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.
References = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/ https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

NEW QUESTION: 88
After a series of account compromises and credential misuse, a company hires a security manager to develop a security program. Which of the following steps should the security manager take first to increase security awareness?
A. Evaluate tools that identify risky behavior and distribute reports on the findings.
B. Develop phishing campaigns and notify the management team of any successes.
C. Update policies and handbooks to ensure all employees are informed of the new procedures.
D. Send quarterly newsletters that explain the importance of password management.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
A company is using a legacy FTP server to transfer financial data to a third party. The legacy system does not support SFTP, so a compensating control is needed to protect the sensitive, financial data in transit. Which of the following would be the most appropriate for the company to use?
A. SSH tunneling
B. Telnet connection
C. Full disk encryption
D. Patch installation

Answer: (SHOW ANSWER)

NEW QUESTION: 90
A growing company would like to enhance the ability of its security operations center to detect threats but reduce the amount of manual work required tor the security analysts. Which of the following would best enable the reduction in manual work?
A. SOAR
B. SIEM
C. MDM
D. DLP
Answer: A (LEAVE A REPLY)
Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

NEW QUESTION: 91
Which of the following threat actors would most likely deface the website of a high-profile music group?
A. Unskilled attacker
B. Organized crime
C. Nation-state
D. Insider threat
Answer: A (LEAVE A REPLY)
Detailed Explanation:An unskilled attacker, often referred to as a script kiddie, is likely to engage in website defacement. This type of attack typically requires minimal expertise and is often conducted for notoriety.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Threat Actors and Motivations".

NEW QUESTION: 92
Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?
A. Business impact analysts
B. Policies and procedures
C. Vulnerability assessment
D. Asset management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
A systems administrator discovers a system that is no longer receiving support from the vendor. However, this system and its environment are critical to running the business, cannot be modified, and must stay online.
Which of the following risk treatments is the most appropriate in this situation?
A. Avoid
B. Transfer
C. Accept
D. Refect
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?
A. Availability
B. Accounting
C. Authentication
D. Authorization
Answer: B (LEAVE A REPLY)
Accounting logs user activities such as log-ins and usage duration, which is part of the AAA framework (Authentication, Authorization, and Accounting).

NEW QUESTION: 95
After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network.
Which of the following is the most appropriate to disable?
A. Console access
B. Routing protocols
C. VLANs

D. Web-based administration

Answer: D (LEAVE A REPLY)

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods.

Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF).

Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs). References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here' s How to Fix It

NEW QUESTION: 96

An organization has recently decided to implement SSO. The requirements are to leverage access tokens and focus on application authorization rather than user authentication. Which of the following solutions would the engineering team most likely configure?

A. LDAP

B. OAuth

C. SAML

D. Federation

Answer: B (LEAVE A REPLY)

NEW QUESTION: 97

Which of the following Is a common, passive reconnaissance technique employed by penetration testers in the early phases of an engagement?

A. Open-source intelligence

B. Exploit validation

C. Pivoting

D. Port scanning

Answer: (SHOW ANSWER)

NEW QUESTION: 98

Which of the following best describes why me SMS DIP authentication method is more risky to implement than the TOTP method?

A. The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.

B. Generally. SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds

C. The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code than the TOTP method.

D. The algorithm used to generate on SMS OTP code is weaker than the one used to generate a TOTP code

Answer: C (LEAVE A REPLY)

The SMS OTP (One-Time Password) method is more vulnerable to interception compared to TOTP (Time- based One-Time Password) because SMS messages can be intercepted through various attack vectors like SIM swapping or SMS phishing. TOTP, on the other hand, generates codes directly on the device and does not rely on a communication channel like SMS, making it less susceptible to interception.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management.

NEW QUESTION: 99

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing

B. Disinformation

C. Impersonating

D. Whaling

Answer: D (LEAVE A REPLY)

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.

NEW QUESTION: 100

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use.

Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

A. Enable SAML

B. Create OAuth tokens.

C. Use password vaulting.
D. Select an IdP
Answer: (SHOW ANSWER)
The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.
Enabling SAML would be part of the technical implementation but comes after selecting an IdP.
OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.
Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

NEW QUESTION: 101
Which of the following should a company use to provide proof of external network security testing?
A. Business impact analysis
B. Supply chain analysis
C. Vulnerability assessment
D. Third-party attestation
Answer: D (LEAVE A REPLY)
Detailed Explanation:Third-party attestation involves an external, independent party performing a network security assessment and providing documented proof, ensuring objectivity and compliance with regulatory or client requirements. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Compliance and Security Audits".

NEW QUESTION: 102
Which of the following is a preventive physical security control?
A. Video surveillance system
B. Alarm system
C. Motion sensors
D. Bollards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
After failing an audit twice, an organization has been ordered by a government regulatory agency to pay fines.
Which of the following caused this action?
A. Rules of engagement
B. Non-compliance
C. Government sanctions

D. Contract violations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following can be used to compromise a system that is running an RTOS?
A. Replay attack
B. Ransomware
C. Memory injection
D. Cross-site scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following actions best addresses a vulnerability found on a company's web server?
A. Patching
B. Decommissioning
C. Segmentation
D. Monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 106
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?
A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 10.50.10.25/32 0.0.0.0
/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0
/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 10.50.10.25
/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0
/0 port 53
Answer: D (LEAVE A REPLY)
A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:
Access list <direction> <action> <source address> <destination address> <protocol> <port> To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only

the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.

NEW QUESTION: 107
A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Select two.)
A. Tokenization
B. Cryptographic downgrade
C. SSH tunneling
D. Segmentation
E. Patch installation
F. Data masking
Answer: C,D (LEAVE A REPLY)
Detailed Explanation:SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Compensating Controls for Legacy Systems".

NEW QUESTION: 108
An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).
A. Application
B. Authentication
C. DHCP
D. Network

E. Firewall
F. Database
Answer: C,E (LEAVE A REPLY)
To identify the impacted host in a command-and-control (C2) server incident, the following logs should be analyzed:
DHCP logs: These logs record IP address assignments. By reviewing DHCP logs, an organization can determine which host was assigned a specific IP address during the time of the attack.
Firewall logs: Firewall logs will show traffic patterns, including connections to external C2 servers. Analyzing these logs helps to identify the IP address and port numbers of the communicating host.
Application, Authentication, and Database logs are less relevant in this context because they focus on internal processes and authentication events rather than network traffic involved in a C2 attack.

NEW QUESTION: 109
Which of the following is the best way to secure an on-site data center against intrusion from an insider?
A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following control types is AUP an example of?
A. Physical
B. Managerial
C. Technical
D. Operational
Answer: B (LEAVE A REPLY)
An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization's operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees.
Physical controls refer to security measures like locks, fences, or security guards.
Technical controls involve security mechanisms such as firewalls or encryption.
Operational controls are procedures for maintaining security, such as backup and recovery plans.

NEW QUESTION: 111

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

A. Business continuity

B. Physical security

C. Change management

D. Disaster recovery

Answer: A (LEAVE A REPLY)

The IT manager is creating a Business Continuity Plan (BCP). A BCP describes how an organization will continue to operate during and after a disaster or global incident. It ensures that critical business functions remain operational despite adverse conditions, with a focus on minimizing downtime and maintaining essential services.

Physical security relates to protecting physical assets.

Change management ensures changes in IT systems are introduced smoothly, without disrupting operations.

Disaster recovery is a subset of business continuity but focuses specifically on recovering from IT-related incidents.

NEW QUESTION: 112

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active

B. Passive

C. Defensive

D. Offensive

Answer: (SHOW ANSWER)

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-
701 Practice Test 1, Question 1.

NEW QUESTION: 113

A systems administrator wants to prevent users from being able to access data based on their responsibilities.
The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?
A. RBAC
B. ACL
C. SAML
D. GPO
Answer: (SHOW ANSWER)
RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

NEW QUESTION: 114
Which of the following is the most relevant reason a DPO would develop a data inventory?
A. To determine the impact in the event of a breach
B. To extend the length of time data can be retained
C. To manage data storage requirements better
D. To automate the reduction of duplicated data
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following would be the best way to test resiliency in the event of a primary power failure?
A. Parallel processing
B. Simulation testing
C. Tabletop exercise
D. Production failover
Answer: D (LEAVE A REPLY)

NEW QUESTION: 116
Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address." Which of the following are the best responses to this situation? (Choose two).
A. Cancel current employee recognition gift cards.

B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.
Answer: B,C (LEAVE A REPLY)
This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money. References = What Is Phishing | Cybersecurity | CompTIA, Phishing - SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

NEW QUESTION: 117
Company A jointly develops a product with Company B, which is located in a different country. Company A finds out that their intellectual property is being shared with unauthorized companies. Which of the following has been breached?
A. SLA
B. AUP
C. SOW
D. MOA
Answer: (SHOW ANSWER)
Detailed Explanation:A Memorandum of Agreement (MOA) outlines terms of cooperation, including restrictions on sharing intellectual property. A breach indicates the terms of the agreement were violated, compromising confidentiality or usage terms. Reference: CompTIA Security+ SY0-701 Study Guide, Domain
5: Security Program Management, Section: "Third-Party Risk Management".

NEW QUESTION: 118
Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?
A. Fines
B. Audit findings
C. Sanctions
D. Reputation damage
Answer: A (LEAVE A REPLY)
PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to

protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.

The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment. B. Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls and recommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non-compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2:

Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8.

PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council], PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question
12. [PCI Security Standards Council], PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council], PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council], PCI DSS FAQs, question
17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council], PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council], PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question
22. [PCI Security Standards Council], PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council], PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council], PCI DSS FAQs, question
27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council], PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

NEW QUESTION: 119
A new vulnerability enables a type of malware that allows the unauthorized movement of data from a system.
Which of the following would detect this behavior?
A. Implementing encryption
B. Monitoring outbound traffic
C. Using default settings
D. Closing all open ports
Answer: B (LEAVE A REPLY)
Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.
References =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

NEW QUESTION: 120
An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?
A. Asset inventory

B. Network enumeration
C. Data certification
D. Procurement process
Answer: A (LEAVE A REPLY)
To ensure that all systems requiring the patch are updated, the systems administrator must maintain an accurate asset inventory. This inventory lists all hardware and software assets within the organization, allowing the administrator to identify which systems are affected by the patch and ensuring that none are missed during the update process.
Network enumeration is used to discover devices on a network but doesn't track software that requires patching.
Data certification and procurement process are unrelated to tracking systems for patching purposes.

NEW QUESTION: 121
Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?
A. Hacktivists
B. Script kiddies
C. Competitors
D. Shadow IT
Answer: (SHOW ANSWER)
Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit IT department approval. This is the most likely cause of introducing vulnerabilities on a corporate network by deploying unapproved software, as such software may not have been vetted for security compliance, increasing the risk of vulnerabilities.
References =
CompTIA Security+ SY0-701 Course Content: The concept of Shadow IT is discussed as a significant risk due to the introduction of unapproved and potentially vulnerable software into the corporate network.

NEW QUESTION: 122
Which of the following security control types does an acceptable use policy best represent?

A. Detective
B. Compensating
C. Corrective
D. Preventive
Answer: D (LEAVE A REPLY)
An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network1.
An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature2.
Some examples of preventive controls are:
Locks, fences, or guards that prevent unauthorized physical access to a facility or a device
Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:
Downloading or installing unauthorized or malicious software
Accessing or sharing sensitive or confidential information without authorization or encryption
Using the network or the system for personal, illegal, or unethical purposes Bypassing or disabling security controls or mechanisms Connecting unsecured or unapproved devices to the network By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions3.
References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

NEW QUESTION: 123
A security officer is implementing a security awareness program and is placing security-themed posters around the building and is assigning online user training. Which of the following would the security officer most likely implement?
A. Phishing campaign
B. Access badges
C. Password policy

D. Risk assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
An organization needs to monitor its users' activities to prevent insider threats. Which of the following solutions would help the organization achieve this goal?
A. Behavioral analytics
B. Access control lists
C. Identity and access management
D. Network intrusion detection system
Answer: A (LEAVE A REPLY)
Detailed Explanation:Behavioral analytics tools monitor user actions and detect anomalies that may indicate insider threats, such as unauthorized access or unusual data exfiltration activities. These tools establish baselines for normal behavior and flag deviations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Behavioral Analytics and Monitoring".

NEW QUESTION: 125
A security analyst is investigating a workstation that is suspected of outbound communication to a command- and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted.
Which of the following logs would the analyst most likely look at next?
A. IPS
B. Firewall
C. ACL
D. Windows security
Answer: B (LEAVE A REPLY)
Since the logs on the endpoint were deleted, the next best option for the analyst is to examine firewall logs.
Firewall logs can reveal external communication, including outbound traffic to a command-and-control (C2) server. These logs would contain information about the IP addresses, ports, and protocols used, which can help in identifying suspicious connections.
IPS logs may provide information about network intrusions, but firewall logs are better for tracking communication patterns.
ACL logs (Access Control List) are useful for tracking access permissions but not for identifying C2 communication.
Windows security logs would have been ideal if they had not been deleted

NEW QUESTION: 126

The internal audit team determines a software application is no longer in scope for external reporting requirements. Which of the following will confirm management's perspective that the application is no longer applicable?

A. Data inventory and retention

B. Right to be forgotten

C. Due care and due diligence

D. Acknowledgement and attestation

Answer: D (LEAVE A REPLY)

Acknowledgement and attestation involve formal confirmation that an application is no longer in scope for compliance, auditing, or reporting requirements. This typically includes documentation signed by relevant stakeholders confirming that the software no longer processes, stores, or transmits relevant data.

* Data inventory and retention (A) is related to managing data assets, not software scope confirmation.

* Right to be forgotten (B) pertains to privacy laws (e.g., GDPR), allowing individuals to request data deletion.

* Due care and due diligence (C) focus on security best practices rather than software applicability.

NEW QUESTION: 127

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage

B. Secure DNS cryptographic downgrade

C. On-path resource consumption

D. Reflected denial of service

Answer: (SHOW ANSWER)

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

NEW QUESTION: 128

An organization has a new regulatory requirement to implement corrective controls on a financial system.
Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: D (LEAVE A REPLY)
Detailed Explanation:
Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Controls for Financial Systems".

NEW QUESTION: 129
Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).
A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor
Answer: (SHOW ANSWER)
Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

NEW QUESTION: 130
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?
A. Virus
B. Trojan
C. Spyware

D. Ransomware

Answer: D (LEAVE A REPLY)

Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.

NEW QUESTION: 131

A certificate authority needs to post information about expired certificates. Which of the following would accomplish this task?

A. TPM

B. CRL

C. PKI

D. CSR

Answer: (SHOW ANSWER)

A Certificate Revocation List (CRL) is a digitally signed list maintained by a Certificate Authority (CA) that contains revoked or expired certificates. This prevents clients from trusting compromised or outdated certificates.

* TPM (A) is a hardware security module, unrelated to certificate revocation.
* PKI (C) is the overall system managing digital certificates, but it does not store revocation lists.
* CSR (D) is a request to obtain a certificate, not to revoke one.

NEW QUESTION: 132

Which of the following activities are associated with vulnerability management? (Select two).

A. Exploiting

B. Prioritization

C. Containment

D. Tabletop exercise

E. Reporting

F. Correlation

Answer: (SHOW ANSWER)

NEW QUESTION: 133

Which of the following describes the maximum allowance of accepted risk?

A. Risk indicator

B. Risk level

C. Risk score

D. Risk threshold

Answer: D (LEAVE A REPLY)

Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
34; Accepting Risk: Definition, How It Works, and Alternatives

NEW QUESTION: 134
A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?
A. Security of cloud providers
B. Cost of implementation
C. Ability of engineers
D. Security of architecture
Answer: D (LEAVE A REPLY)
Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

NEW QUESTION: 135
The management team notices that new accounts that are set up manually do not always have correct access or permissions.
Which of the following automation techniques should a systems administrator use to streamline account creation?
A. Guard rail script
B. Ticketing workflow
C. Escalation script
D. User provisioning script
Answer: D (LEAVE A REPLY)
A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or

permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources12.
The other options are not automation techniques that can streamline account creation:
Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software3.
Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process4.
Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer3: CompTIA Security + SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

NEW QUESTION: 136
An administrator wants to automate an account permissions update for a large number of accounts. Which of the following would best accomplish this task?
A. Federation
B. User provisioning
C. Vertical scaling
D. Security groups
Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
Which of the following data states applies to data that is being actively processed by a database server?

A. In transit
B. Being hashed
C. In use
D. At rest
Answer: (SHOW ANSWER)

NEW QUESTION: 138
The physical security team at a company receives reports that employees are not displaying their badges. The team also observes employees tailgating at controlled entrances. Which of the following topics will the security team most likely emphasize in upcoming security training?
A. Social engineering
B. Situational awareness
C. Phishing
D. Acceptable use policy
Answer: B (LEAVE A REPLY)
Situational awareness refers to being mindful of security risks in one's environment and taking proactive measures to mitigate them. In this scenario, employees are failing to display their identification badges and allowing unauthorized personnel to follow them into restricted areas (tailgating). These behaviors pose significant security risks, such as unauthorized access to sensitive locations.
Security training focused on situational awareness will educate employees on the importance of remaining vigilant about security practices, recognizing potential threats, and enforcing access control measures.
* Social engineering involves manipulating individuals to gain unauthorized access, but this scenario highlights poor adherence to security protocols rather than deception.
* Phishing is an email-based attack aimed at stealing sensitive information, which is unrelated to physical security lapses.
* Acceptable use policy governs the proper use of company resources but does not specifically address tailgating or badge display issues.
Thus, situational awareness is the most relevant security training topic for addressing these concerns.

NEW QUESTION: 139
An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted?
(Choose two.)
A. Typosquatting
B. Phishing
C. Impersonation
D. Vishing

E. Smishing

F. Misinformation

Answer: B,E (LEAVE A REPLY)

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action12. In this scenario, the text message that claims to be from the payroll department is an example of smishing.

Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in- person visits, and can be used to obtain information, access, or money from the victim34. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

A: Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads56. Typosquatting is not related to text messages or credential verification.

B: Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action78. Phishing is not related to text messages or credential verification.

D: Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply9 . Vishing is not related to text messages or credential verification.

F: Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda . Misinformation is not related to text messages or credential verification.

References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3:

Impersonation Attacks: What Are They and How Do You Protect Against Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

NEW QUESTION: 140
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?
A. Compensating control
B. Network segmentation
C. Transfer of risk
D. SNMP traps
Answer: A (LEAVE A REPLY)
A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions:
Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION: 141
Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?
A. Hot site
B. Warm site
C. Cold site
D. Recovery site
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
A company's Chief Information Security Officer (CISO) wants to enhance the capabilities of the incident response team. The CISO directs the incident response team to deploy a tool that rapidly analyzes host and network data from potentially compromised systems and forwards the data for further review. Which of the following tools should the incident response team deploy?
A. NAC
B. IPS

C. SIEM
D. EDR
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
An Endpoint Detection and Response (EDR) solution is designed to monitor, detect, and respond to security incidents on endpoints (such as workstations and servers). It collects and analyzes data, detecting suspicious activity and forwarding relevant information for further investigation.
* Network Access Control (NAC) (A) enforces network access policies but does not analyze security threats on hosts.
* Intrusion Prevention Systems (IPS) (B) detect and block network threats but do not provide deep endpoint analytics.
* Security Information and Event Management (SIEM) (C) aggregates logs and provides security analytics but lacks direct endpoint detection and response capabilities.
EDR is the best choice for analyzing and responding to endpoint security incidents.

NEW QUESTION: 143
An organization is evaluating new regulatory requirements associated with the implementation of corrective controls on a group of interconnected financial systems. Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: B (LEAVE A REPLY)
The primary goal of corrective controls in financial systems is to ensure that errors do not propagate across interconnected systems. Financial transactions are often interdependent, meaning one incorrect or unauthorized change can affect multiple systems. Regulations often mandate these controls to maintain accuracy and prevent cascading failures.
* A (insider threats altering banking details) is a concern, but this scenario focuses on corrective controls, not insider threats specifically.
* C (business insurance) is unrelated to why corrective controls are implemented.
* D (preventing unauthorized changes) falls under preventive, not corrective controls.

NEW QUESTION: 144
A company has yearly engagements with a service provider. The general terms and conditions are the same for all engagements. The company wants to simplify the process and revisit the general terms every three years. Which of the following documents would provide the best way to set the general terms?
A. MSA
B. NDA
C. MOU

D. SLA

Answer: A (LEAVE A REPLY)

A Master Service Agreement (MSA) establishes the general terms and conditions for ongoing business engagements. This allows companies to reuse the same terms across multiple contracts, revisiting them periodically for updates.

* NDA (B) protects confidential information but does not define service terms.
* MOU (C) is a non-binding agreement, often used for partnerships, not formal service contracts.
* SLA (D) focuses on service performance expectations, not overall contract terms.

NEW QUESTION: 145

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Explanation:

Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable

servicesApplication Backdoor Implement 2FA using push notification A screenshot of a computer program Description automatically generated with low confidence

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

NEW QUESTION: 146
Which of the following is best used to detect fraud by assigning employees to different roles?
A. Least privilege
B. Mandatory vacation
C. Separation of duties
D. Job rotation
Answer: D (LEAVE A REPLY)
Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotating roles, organizations can uncover irregularities and discrepancies that might have been concealed by an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization's overall resilience and flexibility.
References =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Risk Management and Compliance.

NEW QUESTION: 147
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?
A. Secured zones
B. Subject role

C. Adaptive identity
D. Threat scope reduction
Answer: D (LEAVE A REPLY)
The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.
One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access.
This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.
The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions.
Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.
References = https://bing.com/search?q=Zero+Trust+data+plane
https://learn.microsoft.com/en-us/security/zero-trust/deploy/data

NEW QUESTION: 148
A systems administrator needs to encrypt all data on employee laptops. Which of the following encryption levels should be implemented?
A. File
B. Volume
C. Full disk
D. Partition
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?
A. Partially known environment
B. Unknown environment
C. Integrated

D. Known environment

Answer: A (LEAVE A REPLY)

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test1.

NEW QUESTION: 150

During a SQL update of a database, a temporary field that was created was replaced by an attacker in order to allow access to the system. Which of the following best describes this type of vulnerability?

A. Side loading

B. Malicious update

C. Memory injection

D. Race condition

Answer: D (LEAVE A REPLY)

NEW QUESTION: 151

An organization is developing a security program that conveys the responsibilities associated with the general operation of systems and software within the organization. Which of the following documents would most likely communicate these expectations?

A. Business continuity plan

B. Change management procedure

C. Acceptable use policy

D. Software development life cycle policy

Answer: (SHOW ANSWER)

Detailed Explanation:

A software development life cycle (SDLC) policy outlines responsibilities, best practices, and standards for developing, deploying, and maintaining secure systems and software. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 5: Security Program Management, Section: "Policies and Standards".

NEW QUESTION: 152
A penetration test identifies that an SMBvl Is enabled on multiple servers across an organization. The organization wants to remediate this vulnerability in the most efficient way possible. Which of the following should the organization use for this purpose?
A. GPO
B. ACL
C. SFTP
D. DLP
Answer: A (LEAVE A REPLY)
"Group Policy Objects (GPOs) are a feature of Microsoft Windows Active Directory that allow administrators to centrally manage and configure settings across multiple systems in an efficient manner. When a vulnerability such as SMBv1 (Server Message Block version 1) is identified on multiple servers, GPOs can be used to disable this outdated and insecure protocol across all affected systems simultaneously. By creating a GPO to enforce a policy that disables SMBv1, the organization can ensure consistent remediation without manually configuring each server individually, making it the most efficient solution for domain-joined environments."

NEW QUESTION: 153
Which of the following is a benefit of an RTO when conducting a business impact analysis?
A. It determines the likelihood of an incident and its cost.
B. It determines the roles and responsibilities for incident responders.
C. It determines the state that systems should be restored to following an incident.
D. It determines how long an organization can tolerate downtime after an incident.
Answer: D (LEAVE A REPLY)
Recovery Time Objective (RTO) defines the maximum acceptable downtime before business operations must be restored. It helps organizations set expectations for recovery speed and prioritize system restoration accordingly.
* A (likelihood of an incident and cost) relates to risk assessment, not RTO.
* B (roles and responsibilities) falls under incident response planning, not RTO.
* C (state of restored systems) is covered by Recovery Point Objective (RPO), not RTO.

NEW QUESTION: 154
The Cruel Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells me analyst the installation must be done as quickly as possible. Which of the following courses of action should the security analyst take first?
A. Log in to the server and perform a health check on the VM.
B. Install the patch Immediately.
C. Confirm that the backup service is running.
D. Take a snapshot of the VM.
Answer: (SHOW ANSWER)

Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.
References = CompTIA Security+ SY0-701 study materials, focusing on change management and backup strategies.

NEW QUESTION: 155
Which of the following is used to validate a certificate when it is presented to a user?
A. OCSP
B. CSR
C. CA
D. CRC
Answer: A (LEAVE A REPLY)
OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 337 1

NEW QUESTION: 156
A customer has a contract with a CSP and wants to identify which controls should be implemented in the IaaS enclave. Which of the following is most likely to contain this information?
A. Statement of work
B. Responsibility matrix
C. Service-level agreement
D. Master service agreement
Answer: B (LEAVE A REPLY)
A responsibility matrix clarifies the division of responsibilities between the cloud service provider (CSP) and the customer, ensuring that each party understands and implements their respective security controls.
References: Security+ SY0-701 Course Content.

NEW QUESTION: 157
Which of the following tools is best for logging and monitoring in a cloud environment?
A. FIM
B. IPS

C. SIEM
D. NAC
Answer: (SHOW ANSWER)

NEW QUESTION: 158
A security administrator needs to reduce the attack surface in the company's data centers. Which of the following should the security administrator do to complete this task?
A. Implement a honeynet.
B. Define Group Policy on the servers.
C. Configure the servers for high availability.
D. Upgrade end-of-support operating systems.
Answer: D (LEAVE A REPLY)
Upgrading end-of-support operating systems is one of the most effective ways to reduce the attack surface. Unsupported OS versions no longer receive security patches, making them prime targets for attackers. Removing outdated software ensures that known vulnerabilities cannot be exploited.
* A (honeynet) is used for threat analysis, not reducing the attack surface.
* B (Group Policy) helps enforce security policies but does not address outdated vulnerabilities.
* C (High availability) focuses on uptime, not security risk reduction.

NEW QUESTION: 159
While investigating a possible incident, a security analyst discovers the following log entries:
67.118.34.157 ----- [28/Jul/2022:10:26:59 -0300] "GET /query.php?q-wireless%20headphones / HTTP/1.0"
200 12737
132.18.222.103 ----[28/Jul/2022:10:27:10 -0300] "GET /query.php?q=123 INSERT INTO users VALUES ('temp', 'pass123')# / HTTP/1.0" 200 935
12.45.101.121 ----- [28/Jul/2022:10:27:22 -0300] "GET /query.php?q=mp3%20players I HTTP/1.0" 200
14650
Which of the following should the analyst do first?
A. Implement a WAF
B. Disable the query .php script
C. Block brute-force attempts on temporary users
D. Check the users table for new accounts
Answer: D (LEAVE A REPLY)
The logs show an SQL injection attack. The first step is to verify if new accounts have been created, indicating a successful injection.

NEW QUESTION: 160

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

A. Code scanning for vulnerabilities

B. Open-source component usage

C. Quality assurance testing

D. Peer review and approval

Answer: (SHOW ANSWER)

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

NEW QUESTION: 161

Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption

B. Hashing

C. Data masking

D. Steganography

Answer: D (LEAVE A REPLY)

Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key. Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software12

NEW QUESTION: 162

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.

Which of the following analysis elements did the company most likely use in making this decision?

A. IMTTR

B. RTO

C. ARO

D. MTBF

Answer: C (LEAVE A REPLY)

ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and

management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.
The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.
IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team.
RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption.
RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 97-98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

NEW QUESTION: 163
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?
A. SCAP
B. Net Flow
C. Antivirus
D. DLP
Answer: (SHOW ANSWER)
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the

recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets.
References = CompTIA Security+ Study Guide with over 500 Practice Test Questions:
Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain
2.5, page 11.

NEW QUESTION: 164
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
. Something you know
. Something you have
. Something you are
Which of the following would accomplish the manager's goal?
A. Domain name, PKI, GeoIP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address
Answer: C (LEAVE A REPLY)
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.
Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12 Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12 Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12

NEW QUESTION: 165
A new security regulation was announced that will take effect in the coming year. A company must comply with it to remain in business. Which of the following activities should the company perform next?
A. Security procedure evaluation
B. Threat scope reduction
C. Policy review

D. Gap analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access? 1
A. Role-based
B. Least privilege
C. Discretionary
D. Time of day
Answer: A (LEAVE A REPLY)

NEW QUESTION: 167
A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?
A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors
Answer: A (LEAVE A REPLY)
Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability12. Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it3. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:

Establishing a trusted relationship with the OEM and authorized resellers Requesting documentation and certification of the hardware from the OEM or authorized resellers Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components Testing the hardware for functionality, performance, and security Implementing a tracking system to monitor the hardware throughout its lifecycle Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security?
Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, :
Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION: 168
A company is working with a vendor to perform a penetration test Which of the following includes an estimate about the number of hours required to complete the engagement?
A. SOW
B. BPA
C. SLA
D. NDA
Answer: (SHOW ANSWER)
A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 492; What to Look For in a Penetration Testing Statement of Work?

NEW QUESTION: 169
Which of the following can a security director use to prioritize vulnerability patching within a company's IT environment?
A. SOAR
B. CVSS
C. SIEM
D. CVE
Answer: B (LEAVE A REPLY)
The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities. It helps organizations prioritize vulnerability patching by providing a numerical score that reflects the potential impact and exploitability of a vulnerability.

CVSS scores are used to gauge the urgency of patching vulnerabilities within a company's IT environment.
References =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Vulnerability Management.

NEW QUESTION: 170
A security analyst receives an alert from a corporate endpoint used by employees to issue visitor badges. The alert contains the following details:
Which of the following best describes the indicator that triggered the alert?
A. Blocked content
B. Brute-force attack
C. Concurrent session usage
D. Account lockout
Answer: B (LEAVE A REPLY)
Detailed Explanation:The activity described in the table, where multiple connection attempts are made on port
445 (used for SMB services), suggests a brute-force attack. The attacker likely used automated methods to guess credentials, causing multiple failures. Such attempts are a hallmark of brute-force attacks targeting shared resources. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Indicators of Malicious Activity".

NEW QUESTION: 171
Which of the following actions must an organization take to comply with a person's request for the right to be forgotten?
A. Purge all personally identifiable attributes.
B. Encrypt all of the data.
C. Remove all of the person's data.
D. Obfuscate all of the person's data.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
The right to be forgotten, as outlined in regulations such as the General Data Protection Regulation (GDPR), requires organizations to permanently delete an individual's personal data upon request, unless there is a legal or contractual obligation to retain it.
* Purging personally identifiable attributes (A) removes some identifying data but does not fully satisfy the request.
* Encrypting the data (B) does not remove it, and the data is still accessible with the decryption key.
* Obfuscating data (D) makes data unreadable but does not permanently remove it.

To comply with the right to be forgotten, organizations must remove all of the person's data unless an exception applies.

NEW QUESTION: 172
An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?
A. Compromise
B. Retention
C. Analysis
D. Transfer
E. Inventory
Answer: B (LEAVE A REPLY)
A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.
References
CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211
CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

NEW QUESTION: 173
Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?
A. Data sovereignty
B. Data segmentation
C. Geographic restrictions
D. Geographic dispersion
Answer: A (LEAVE A REPLY)

NEW QUESTION: 174
A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data.
Which of the following should the administrator do first?
A. Block access to cloud storage websites.
B. Create a rule to block outgoing email attachments.
C. Apply classifications to the data.
D. Remove all user permissions from shares on the file server.

Answer: C (LEAVE A REPLY)
Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk.
Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page
327.

NEW QUESTION: 175
Which of the following is the stage in an investigation when forensic images are obtained?
A. Acquisition
B. Preservation
C. Reporting
D. E-discovery
Answer: A (LEAVE A REPLY)
Detailed Explanation:The acquisition phase involves creating forensic images (exact replicas) of storage devices or memory to ensure data integrity for further analysis. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Forensic Imaging and Chain of Custody".

NEW QUESTION: 176
An administrator is reviewing a single server's security logs and discovers the following; Which of the following best describes the action captured in this log file?
A. Brute-force attack
B. Privilege escalation
C. Failed password audit
D. Forgotten password by the user
Answer: (SHOW ANSWER)
A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

NEW QUESTION: 177

In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective. Which of the following best describes the security engineer's response?

A. Risk tolerance

B. Risk acceptance

C. Risk importance

D. Risk appetite

Answer: D (LEAVE A REPLY)

Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

NEW QUESTION: 178

Which of the following organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?

A. MOA

B. EULA

C. AUP

D. SLA

Answer: (SHOW ANSWER)

NEW QUESTION: 179

An organization's web servers host an online ordering system. The organization discovers that the servers are vulnerable to a malicious JavaScript injection, which could allow attackers to access customer payment information. Which of the following mitigation strategies would be most effective for preventing an attack on the organization's web servers? (Select two).

A. Regularly updating server software and patches

B. Utilizing a web-application firewall

C. Removing payment information from the servers

D. Performing regular vulnerability scans

E. Implementing strong password policies

F. Encrypting sensitive data at rest and in transit

Answer: (SHOW ANSWER)

NEW QUESTION: 180

While reviewing logs, a security administrator identifies the following code:

<script>function(send_info)</script>
Which of the following best describes the vulnerability being exploited?
A. CSRF
B. XSS
C. DDoS
D. SQLi
Answer: B (LEAVE A REPLY)

NEW QUESTION: 181
During a penetration test, a vendor attempts to enter an unauthorized area using an access badge Which of the following types of tests does this represent?
A. Defensive
B. Passive
C. Offensive
D. Physical
Answer: D (LEAVE A REPLY)
Attempting to enter an unauthorized area using an access badge during a penetration test is an example of a physical test. This type of test evaluates the effectiveness of physical security controls, such as access badges, security guards, and locks, in preventing unauthorized access to restricted areas.
Defensive and offensive testing typically refer to digital or network-based penetration testing strategies.
Passive testing involves observing or monitoring but not interacting with the environment.

NEW QUESTION: 182
In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?
A. Key stretching
B. Tokenization
C. Data masking
D. Salting
Answer: D (LEAVE A REPLY)

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting.
This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables.References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 183
While investigating a recent security breach an analyst finds that an attacker gained access by SOL infection through a company website. Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?
A. Secure cookies
B. Input sanitization
C. Code signing
D. Blocklist
Answer: B (LEAVE A REPLY)
Input sanitization is a critical security measure to prevent SQL injection attacks, which occur when an attacker exploits vulnerabilities in a website's input fields to execute malicious SQL code. By properly sanitizing and validating all user inputs, developers can prevent malicious code from being executed, thereby securing the website against such attacks.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common vulnerability mitigation strategies.

NEW QUESTION: 184
One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?
A. Virtualization
B. Firmware
C. Application
D. Operating system
Answer: B (LEAVE A REPLY)
Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

NEW QUESTION: 185
Which of the following allows for the attribution of messages to individuals?
A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs
Answer: B (LEAVE A REPLY)
Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document. References = Non-repudiation - CompTIA Security+ SY0-701 - 1.2, CompTIA Security+ SY0-301: 6.1 - Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

NEW QUESTION: 186
During a recent log review, an analyst discovers evidence of successful injection attacks. Which of the following will best address this issue?
A. Authentication
B. Secure cookies
C. Static code analysis
D. Input validation
Answer: D (LEAVE A REPLY)
Input validation is the primary defense against injection attacks, such as SQL injection or command injection. It ensures that user-supplied data is properly sanitized before processing, preventing attackers from injecting malicious code.
* Authentication (A) helps verify user identity but does not prevent injection attacks.
* Secure cookies (B) improve session security but do not address injection vulnerabilities.
* Static code analysis (C) helps identify vulnerabilities in source code but does not actively prevent attacks in real-time.

NEW QUESTION: 187
Which of the following is the most common data loss path for an air-gapped network?
A. Bastion host
B. Unsecured Bluetooth
C. Unpatched OS
D. Removable devices
Answer: (SHOW ANSWER)
An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can

still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

NEW QUESTION: 188
A company wants to ensure employees are allowed to copy files from a virtual desktop during the workday but are restricted during non-working hours. Which of the following security measures should the company set up?
A. Digital rights management
B. Time-based access control
C. Network access control
D. Role-based access control
Answer: (SHOW ANSWER)

NEW QUESTION: 189
A security analyst learns that an attack vector, used as part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of the initial exploit. Which of the following logs should the analyst review first?
A. Endpoint
B. Application
C. Firewall
D. NAC
Answer: (SHOW ANSWER)
Detailed Explanation:Firewall logs provide details of all network traffic, including connections to and from IoT devices. They are typically the first source of evidence for identifying the time of an exploit. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

NEW QUESTION: 190
Which of the following is die most important security concern when using legacy systems to provide production service?
A. Instability
B. Lack of vendor support
C. Loss of availability
D. Use of insecure protocols
Answer: B (LEAVE A REPLY)

The most important security concern when using legacy systems is the lack of vendor support. Without support from the vendor, systems may not receive critical security patches and updates, leaving them vulnerable to exploitation. This lack of support can result in increased risk of security breaches, as vulnerabilities discovered in the software may never be addressed.
References = CompTIA Security+ SY0-701 study materials, particularly in the context of risk management and the challenges posed by legacy systems.

NEW QUESTION: 191
A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?
A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.
Answer: C (LEAVE A REPLY)
After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.
Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.
A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.

Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

NEW QUESTION: 192
Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?
A. Deploy a SIEM solution
B. Create custom scripts to aggregate and analyze logs
C. Implement EDR technology
D. Install a unified threat management appliance
Answer: A (LEAVE A REPLY)
Deploying a Security Information and Event Management (SIEM) solution allows for efficient log aggregation, correlation, and analysis across an organization's infrastructure, providing real-time security insights.References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 193
Which of the following can be used to identify potential attacker activities without affecting production servers?
A. Honey pot
B. Video surveillance
C. Zero Trust
D. Geofencing
Answer: A (LEAVE A REPLY)
A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources12.
The other options are not effective ways to identify potential attacker activities without affecting production servers:
Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers3.

Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers4.
Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers5.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception - SY0-601 CompTIA Security+ : 2.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985:
CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION: 194
A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?
A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software
Answer: C (LEAVE A REPLY)
A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

NEW QUESTION: 195
The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?
A. Penetration test
B. Internal audit
C. Attestation
D. External examination
Answer: D (LEAVE A REPLY)
An external examination (also known as an external audit or external review) is the best method for the Chief Information Security Officer (CISO) to gain an understanding of how the company's

security policies compare to external regulatory requirements. External examinations are conducted by third-party entities that assess an organization's compliance with laws, regulations, and industry standards.
Penetration tests focus on identifying vulnerabilities, not compliance.
Internal audits assess internal controls but are not impartial or focused on regulatory requirements.
Attestation is a formal declaration but does not involve the actual evaluation of compliance.

NEW QUESTION: 196
A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?
A. SSO
B. LEAP
C. MFA
D. PEAP
Answer: (SHOW ANSWER)
SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
B: LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4.
C: MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
D: PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.
References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4:

Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

NEW QUESTION: 197
Which of the following allows a systems administrator to tune permissions for a file?
A. Patching
B. Access control list
C. Configuration enforcement
D. Least privilege
Answer: B (LEAVE A REPLY)
Detailed Explanation:Access control lists (ACLs) allow administrators to fine-tune file permissions by specifying which users or groups have access to a file and defining the level of access.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Mechanisms".

NEW QUESTION: 198
Which of the following best protects sensitive data in transit across a geographically dispersed Infrastructure?
A. Tokenization
B. Masking
C. Encryption
D. Obfuscation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 199
A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?
A. To reduce implementation cost
B. To identify complexity
C. To remediate technical debt
D. To prevent a single point of failure

Answer: D (LEAVE A REPLY)
Ensuring that other team members understand how a script works is essential to prevent a single point of failure. If only one person knows how the script operates, the organization risks being unable to maintain or troubleshoot it if that person is unavailable. Sharing knowledge ensures continuity and reduces dependence on one individual.
Reducing implementation cost and remediating technical debt are secondary considerations in this context.
Identifying complexity is important, but the main benefit is to avoid a single point of failure.

NEW QUESTION: 200
Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?
A. Development
B. Test
C. Production
D. Staging
Answer: D (LEAVE A REPLY)
A staging environment is a controlled setting that closely mirrors the production environment but uses a subset of customer data. It is used to test major system upgrades, assess their impact, and demonstrate new features before they are rolled out to the live production environment. This ensures that any issues can be identified and addressed in a safe environment before affecting end-users.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of secure system development and testing environments.

NEW QUESTION: 201
Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?
A. Encryption
B. Hashing
C. Masking
D. Tokenization
Answer: C (LEAVE A REPLY)
Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

NEW QUESTION: 202

An IT security team is concerned about the confidentiality of documents left unattended in MFPs. Which of the following should the security team do to mitigate the situation?
A. Educate users about the importance of paper shredder devices.
B. Deploy an authentication factor that requires In-person action before printing.
C. Install a software client m every computer authorized to use the MFPs.
D. Update the management software to utilize encryption.
Answer: B (LEAVE A REPLY)
To mitigate the risk of confidential documents being left unattended in Multi-Function Printers (MFPs), implementing an authentication factor that requires in-person action before printing (such as PIN codes or badge scanning) is the most effective measure. This ensures that documents are only printed when the authorized user is present to collect them, reducing the risk of sensitive information being exposed.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of physical security and access control.

NEW QUESTION: 203
Which of the following most accurately describes the order in which a security engineer should implement secure baselines?
A. Deploy, maintain, establish
B. Establish, maintain, deploy
C. Establish, deploy, maintain
D. Deploy, establish, maintain
Answer: C (LEAVE A REPLY)
Detailed Explanation:The correct sequence is to first establish secure baselines by determining the required configurations, deploy those configurations across systems, and finally maintain the configurations through regular updates and auditing. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Secure Baseline Development".

NEW QUESTION: 204
An employee emailed a new systems administrator a malicious web link and convinced the administrator to change the email server's password. The employee used this access to remove the mailboxes of key personnel.
Which of the following security awareness concepts would help prevent this threat in the future?
A. Using password management
B. Recognizing phishing
C. Providing situational awareness training
D. Reviewing email policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 205

A recent penetration test identified that an attacker could flood the MAC address table of network switches.
Which of the following would best mitigate this type of attack?
A. Load balancer
B. Port security
C. IPS
D. NGFW
Answer: B (LEAVE A REPLY)
Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.
Load balancer distributes network traffic but does not address MAC flooding attacks.
IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.
NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC table security.

NEW QUESTION: 206
A university employee logged on to the academic server and attempted to guess the system administrators' log- in credentials. Which of the following security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?
A. Firewall
B. Two-factor authentication
C. Intrusion prevention system
D. User activity logs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 207
Which of the following describes the category of data that is most impacted when it is lost?
A. Public
B. Critical
C. Confidential
D. Private
Answer: (SHOW ANSWER)

NEW QUESTION: 208
A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network.

Which of the following should be configured on the existing network infrastructure to best prevent this activity?

A. Port security

B. Web application firewall

C. Transport layer security

D. Virtual private network

Answer: A (LEAVE A REPLY)

Port security is the best solution to prevent unauthorized devices, like a visitor's laptop, from connecting to the company's network. Port security can limit the number of devices that can connect to a network switch port and block unauthorized MAC addresses, effectively stopping unauthorized access attempts.

Web application firewall (WAF) protects against web-based attacks, not unauthorized network access.

Transport Layer Security (TLS) ensures encrypted communication but does not manage physical network access.

Virtual Private Network (VPN) secures remote connections but does not control access through physical network ports.

NEW QUESTION: 209

An employee who was working remotely lost a mobile device containing company data. Which of the following provides the best solution to prevent future data loss?

A. DLP

B. EDR

C. FDE

D. MDM

Answer: D (LEAVE A REPLY)

NEW QUESTION: 210

An enterprise security team is researching a new security architecture to better protect the company's networks and applications against the latest cyberthreats. The company has a fully remote workforce. The solution should be highly redundant and enable users to connect to a VPN with an integrated, software-based firewall. Which of the following solutions meets these requirements?

A. SASE

B. IPS

C. SIEM

D. CASB

Answer: C (LEAVE A REPLY)

NEW QUESTION: 211

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

A. Local data protection regulations

B. Risks from hackers residing in other countries

C. Impacts to existing contractual obligations

D. Time zone differences in log correlation

Answer: A (LEAVE A REPLY)

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders.

Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States.

A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage.

Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269.

CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

NEW QUESTION: 212

Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?

A. Software development life cycle

B. Risk tolerance

C. Certificate signing request

D. Maintenance window

Answer: (SHOW ANSWER)

NEW QUESTION: 213
A systems administrator is redesigning now devices will perform network authentication. The following requirements need to be met:
* An existing Internal certificate must be used.
* Wired and wireless networks must be supported
* Any unapproved device should be Isolated in a quarantine subnet
* Approved devices should be updated before accessing resources
Which of the following would best meet the requirements?
A. 802.IX
B. EAP
C. RADIUS
D. WPA2
Answer: A (LEAVE A REPLY)
802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

NEW QUESTION: 214
Which of the following should be used to ensure an attacker is unable to read the contents of a mobile device's drive if the device is lost?
A. TPM
B. ECC
C. FDE
D. HSM
Answer: (SHOW ANSWER)
Full Disk Encryption (FDE) ensures that all data on the drive is encrypted, preventing unauthorized access even if the device is lost.

NEW QUESTION: 215
Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Select two).
A. Increased compartmentalization of the system
B. Reduced complexity of the system
C. Easter debugging of the system
D. Improved scalability of the system
E. Stronger authentication of the system

F. Reduced cost of ownership of the system
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 216
An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message.
Which of the following types of social engineering attacks occurred?
A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing
Answer: D (LEAVE A REPLY)
Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one.
The employee entered the log-in information, but received a "page not found" error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website. References = Other Social Engineering Attacks - CompTIA Security+ SY0-701 - 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

NEW QUESTION: 217
An organization wants to improve the company's security authentication method for remote employees. Given the following requirements:
* Must work across SaaS and internal network applications
* Must be device manufacturer agnostic
* Must have offline capabilities
Which of the following would be the most appropriate authentication method?
A. SMS verification
B. Biometrics
C. Username and password
D. Time-based tokens
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

A. Deploy multifactor authentication.

B. Decrease the level of the web filter settings

C. Implement security awareness training.

D. Update the acceptable use policy

Answer: C (LEAVE A REPLY)

In this scenario, employees are attempting to navigate to spoofed websites, which is being blocked by the web filter. To address this issue, the administrator should implement security awareness training. Training helps employees recognize phishing and other social engineering attacks, reducing the likelihood that they will attempt to access malicious websites in the future.

Deploying multifactor authentication (MFA) would strengthen authentication but does not directly address user behavior related to phishing websites.

Decreasing the level of the web filter would expose the organization to more threats.

Updating the acceptable use policy may clarify guidelines but is not as effective as hands-on training for improving user behavior.

NEW QUESTION: 219

An organization maintains intellectual property that it wants to protect. Which of the following concepts would be most beneficial to add to the company's security awareness training program?

A. Phishing awareness

B. Business continuity planning

C. Insider threat detection

D. Simulated threats

Answer: C (LEAVE A REPLY)

NEW QUESTION: 220

Which of the following must be considered when designing a high-availability network? (Choose two).

A. Ease of recovery

B. Ability to patch

C. Physical isolation

D. Responsiveness

E. Attack surface

F. Extensible authentication

Answer: A,E (LEAVE A REPLY)

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:

Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.
The other options are not directly related to high-availability network design:
Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
Responsiveness: This refers to the speed and quality of the network's performance and service delivery.
Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

NEW QUESTION: 221
A company's website is www. Company. com Attackers purchased the domain wwww. company.com Which of the following types of attacks describes this example?
A. Typosquatting
B. Brand Impersonation
C. On-path
D. Watering-hole
Answer: A (LEAVE A REPLY)
"Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register 'wwww.company.com' to mimic 'www.company.
com,' tricking users who mistype the URL into visiting a malicious site. This attack exploits human error and can be used to steal credentials, distribute malware, or impersonate the legitimate entity."

NEW QUESTION: 222
Which of the following methods would most likely be used to identify legacy systems?
A. Bug bounty program
B. Vulnerability scan
C. Package monitoring
D. Dynamic analysis
Answer: B (LEAVE A REPLY)
A vulnerability scan is the most likely method to identify legacy systems. These scans assess an organization's network and systems for known vulnerabilities, including outdated or unsupported software (i.e., legacy systems) that may pose a security risk. The scan results can highlight systems that are no longer receiving updates, helping IT teams address these risks.
Bug bounty programs are used to incentivize external researchers to find security flaws, but they are less effective at identifying legacy systems.
Package monitoring tracks installed software packages for updates or issues but is not as comprehensive for identifying legacy systems.
Dynamic analysis is typically used for testing applications during runtime to find vulnerabilities, but not for identifying legacy systems.

NEW QUESTION: 223
Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls lo a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed. Which of the following is the most likely explanation?
A. The executive team is traveling internationally and trying to avoid roaming charges
B. The company's SIP server security settings are weak.
C. Disgruntled employees are making calls to the partner organization.
D. The service provider has assigned multiple companies the same numbers
Answer: B (LEAVE A REPLY)
If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.
References = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

NEW QUESTION: 224
Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?
A. Continuity of operations
B. Capacity planning

C. Tabletop exercise
D. Parallel processing
Answer: C (LEAVE A REPLY)
A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.
Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.
Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.
Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

NEW QUESTION: 225
A company relies on open-source software libraries to build the software used by its customers. Which of the following vulnerability types would be the most difficult to remediate due to the company's reliance on open- source libraries?
A. Buffer overflow
B. SQL injection
C. Cross-site scripting
D. Zero day
Answer: D (LEAVE A REPLY)
Zero-day vulnerabilities are unknown flaws in software, making them harder to patch, especially when using open-source libraries without dedicated support teams.

NEW QUESTION: 226
An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?
A. Hardening
B. Employee monitoring
C. Configuration enforcement
D. Least privilege
Answer: (SHOW ANSWER)
The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices.

However, it is rarely implemented in practice.
In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.
The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.
References =
https://en.wikipedia.org/wiki/Principle_of_least_privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

NEW QUESTION: 227
An IT administrator needs to ensure data retention standards are implemented on an enterprise application.
Which of the Mowing describes the administrator's role?
A. Privacy officer
B. Custodian
C. Processor
D. Owner
Answer: D (LEAVE A REPLY)

NEW QUESTION: 228
A spoofed identity was detected for a digital certificate. Which of the following are the type of unidentified key and the certificate mat could be in use on the company domain?
A. Private key and root certificate
B. Public key and expired certificate

C. Private key and self-signed certificate
D. Public key and wildcard certificate
Answer: C (LEAVE A REPLY)
A self-signed certificate is a certificate that is signed by its own private key rather than by a trusted certificate authority (CA). This means that the authenticity of the certificate relies solely on the issuer's own authority. If a spoofed identity was detected, it could indicate that a private key associated with a self-signed certificate was compromised. Self-signed certificates are often used internally within organizations, but they carry higher risks since they are not validated by a third-party CA, making them more susceptible to spoofing.
References = CompTIA Security+ SY0-701 study materials, particularly the domains discussing Public Key Infrastructure (PKI) and certificate management.

NEW QUESTION: 229
Which of the following must be considered when designing a high-availability network? (Select two).
A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication
Answer: A,E (LEAVE A REPLY)
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.
Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.
Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

NEW QUESTION: 230

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

A. Deploying a SASE solution to remote employees

B. Building a load-balanced VPN solution with redundant internet

C. Purchasing a low-cost SD-WAN solution for VPN traffic

D. Using a cloud provider to create additional VPN concentrators

Answer: A (LEAVE A REPLY)

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions. References: CompTIA Security+ Study Guide: Exam SY0-
701, 9th Edition, page 457-458 1

NEW QUESTION: 231

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

A. Send out periodic security reminders.

B. Update the content of new hire documentation.

C. Modify the content of recurring training.D Implement a phishing campaign

Answer: C (LEAVE A REPLY)

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701,
9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION: 232

Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking
D. Side loading
Answer: D (LEAVE A REPLY)
Side loading refers to the process of installing applications on a device from outside the official app store, which can introduce security vulnerabilities by bypassing standard app validation processes.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 233
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?
A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading
Answer: D (LEAVE A REPLY)
Side loading is the process of installing software outside of a manufacturer's approved software repository.
This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access.
Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloading - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

NEW QUESTION: 234
Which of the following provides the details about the terms of a test with a third-party penetration tester?
A. Rules of engagement
B. Supply chain analysis
C. Right to audit clause
D. Due diligence
Answer: A (LEAVE A REPLY)
Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:

The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
The testing team credentials and the authorized tools and techniques that they can use.
The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non- disclosure agreements for the test results.
The timeline and duration of the test, and the hours of operation and testing windows.
The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.
Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third- party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.
References = https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of- engagement/
https://bing.com/search?q=rules+of+engagement+penetration+testing

NEW QUESTION: 235
An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Select two).
A. Requiring passwords with eight characters
B. Personal application store access
C. Remote wiping of the device
D. Employee data ownership
E. Data usage caps
F. Data encryption
Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 236
A network engineer is increasing the overall security of network devices and needs to harden the devices.
Which of the following will best accomplish this task?
A. Enabling HTTP administration
B. Replacing Telnet with SSH
C. Configuring centralized logging

D. Generating local administrator accounts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 237
Which of the following would be best suited for constantly changing environments?
A. RTOS
B. Containers
C. Embedded systems
D. SCADA
Answer: B (LEAVE A REPLY)
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION: 238
A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?
A. MSA
B. SLA
C. BPA
D. SOW
Answer: D (LEAVE A REPLY)
An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome.
For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training.
The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the

metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer's CompTIA SY0-701 Security + Training Course, Section 8.2:
Compliance and Controls, video: Contracts and Agreements (5:12).

NEW QUESTION: 239
An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?
A. Tokenization
B. Hashing
C. Obfuscation
D. Segmentation
Answer: (SHOW ANSWER)
To limit the potential impact on the log-in database in case of a breach, the security team would most likely recommend hashing. Hashing converts passwords into fixed-length strings of characters, which cannot be easily reversed to reveal the original passwords. Even if the database is breached, attackers cannot easily retrieve the actual passwords if they are properly hashed (especially with techniques like salting).
Tokenization is used to replace sensitive data with a token, but it is more common for protecting credit card data than passwords.
Obfuscation is the process of making data harder to interpret but is weaker than hashing for password protection.
Segmentation helps isolate data but doesn't directly protect the contents of the login database.

NEW QUESTION: 240
After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?
A. Bluetooth
B. Wired
C. NFC
D. SCADA
Answer: (SHOW ANSWER)
A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is

trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network12.

NEW QUESTION: 241
Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
A. Lead a simulated failover.
B. Conduct a tabletop exercise.
C. Periodically test the generators.
D. Develop requirements for database encryption.
Answer: A (LEAVE A REPLY)
Detailed Explanation:A simulated failover tests the disaster recovery site's ability to handle a full transition of services. This ensures all systems can function as expected during an actual disaster. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Disaster Recovery and Business Continuity Planning".

NEW QUESTION: 242
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?
A. Disaster recovery plan
B. Incident response procedure
C. Business continuity plan
D. Change management procedure
Answer: D (LEAVE A REPLY)
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network.

Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:
A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.
A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.
A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.
A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.
A change documentation that records the details and status of the change, as well as the lessons learned and best practices.
A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.
A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:
Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.
Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.
Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.
Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.
The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-
701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

NEW QUESTION: 243
An employee in the accounting department receives an email containing a demand for payment tot services performed by a vendor However, the vendor is not in the vendor management database. Which of the following in this scenario an example of?
A. Pretexting
B. Impersonation
C. Ransomware
D. Invoice scam
Answer: D (LEAVE A REPLY)
The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non-existent services. These scams often rely on social engineering tactics to bypass financial controls.
References = CompTIA Security+ SY0-701 study materials, particularly in the context of social engineering attacks and common scams.

NEW QUESTION: 244
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?
A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN
Answer: A (LEAVE A REPLY)
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications.
Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor

also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications.
Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud- based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.
SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00;
[Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

NEW QUESTION: 245
Which of the following is required for an organization to properly manage its restore process in the event of system failure?
A. IRP
B. DRP
C. RPO
D. SDLC
Answer: B (LEAVE A REPLY)
A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:
A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
A business impact analysis that prioritizes the recovery of the most essential functions and data.
A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and

minimizing the downtime and data loss. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

NEW QUESTION: 246
Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?
A. Risk mitigation
B. Risk identification
C. Risk treatment
D. Risk monitoring and review
Answer: B (LEAVE A REPLY)
Risk identification is the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includes identifying assets, evaluating threats, and assessing potential vulnerabilities.
* Risk mitigation: Reducing risk by implementing controls.
* Risk treatment: Determining how to handle identified risks.
* Risk monitoring and review: Ongoing evaluation of risk controls.

NEW QUESTION: 247
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?
A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length
Answer: (SHOW ANSWER)
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server. References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1