CompTIA.SY0-701.v2026-07-15.q325

Exam Code:	SY0-701
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	325
Version:	v2026-07-15
# of views:	174
# of Questions views:	3250
https://www.freepdfdumps.com/CompTIA.SY0-701.v2026-07-15.q325.html	

NEW QUESTION: 1
Which of the following is the final step of the modem response process?
A. Lessons learned
B. Eradication
C. Containment
D. Recovery
Answer: A (LEAVE A REPLY)
The final step in the incident response process is "Lessons learned." This step involves reviewing and analyzing the incident to understand what happened, how it was handled, and what could be improved. The goal is to improve future response efforts and prevent similar incidents from occurring. It's essential for refining the incident response plan and enhancing overall security posture.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of incident response and recovery.

NEW QUESTION: 2
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: (SHOW ANSWER)
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues.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.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain
3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective:
Legacy systems 2

NEW QUESTION: 3
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. $30,000
B. $15,000
C. $10,000
D. $7,500
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
A cybersecurity incident response team at a large company receives notification that malware is present on several corporate desktops No known Indicators of compromise have been found on the network. Which of the following should the team do first to secure the environment?
A. Contain the Impacted hosts
B. Add the malware to the application blocklist.
C. Segment the core database server.
D. Implement firewall rules to block outbound beaconing
Answer: A (LEAVE A REPLY)
The first step in responding to a cybersecurity incident, particularly when malware is detected, is to contain the impacted hosts. This action prevents the spread of malware to other parts of the network, limiting the potential damage while further investigation and remediation actions are planned.
References = CompTIA Security+ SY0-701 study materials, particularly on incident response procedures and the importance of containment in managing security incidents.

NEW QUESTION: 5
A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?
A. Hashing
B. Tokenization
C. Encryption

D. Segmentation

Answer: (SHOW ANSWER)

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext. Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data. Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing, tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security. Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

NEW QUESTION: 6

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. Data retention

B. Sanitation

C. Certification

D. Destruction

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

A security analyst is examining a penetration test report and notices that the tester pivoted to critical internal systems with the same local user ID and password. Which of the following would help prevent this in the future?

A. Implement centralized authentication with proper password policies

B. Add password complexity rules and increase password history limits

C. Connect the systems to an external authentication server

D. Limit the ability of user accounts to change passwords

Answer: A (LEAVE A REPLY)

Centralized authentication (such as Active Directory or LDAP) combined with proper password policies helps prevent the reuse of the same local credentials across multiple systems, reducing the risk of lateral movement during attacks like credential reuse or pass-the-hash.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Centralized authentication and strong password policies reduce risks associated with local account reuse." Exam Objectives 3.1: "Implement secure network architecture concepts."

NEW QUESTION: 8

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: 9
Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?
A. Wipe tool
B. Retention platform
C. Degaussing
D. Drive shredder
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following is a prerequisite for a DLP solution?
A. Data destruction
B. Data sanitization
C. Data classification
D. Data masking
Answer: (SHOW ANSWER)
Data classification is required before implementing a Data Loss Prevention (DLP) solution because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.
Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.
Data classification is emphasized in Security Program Management and Data Protection topics#6:Chapter
16 CompTIA Security+ Study Guide#.

NEW QUESTION: 11
A user sends an email that includes a digital signature for validation. Which of the following security concepts would ensure that a user cannot deny that they sent the email?
A. Non-repudiation
B. Confidentiality
C. Integrity
D. Authentication
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:

Non-repudiation ensures that a sender cannot deny sending a message. Digital signatures provide non- repudiation because they use the sender's private key, which only the legitimate owner possesses. When the email recipient verifies the digital signature using the sender's public key, it proves the email was sent by the true owner of the private key and has not been altered.
Confidentiality (B) ensures information is protected from unauthorized access and is usually achieved through encryption. Integrity (C) ensures data has not been modified, while authentication (D) verifies the identity of a user. Although digital signatures also support integrity and authentication, the specific property that prevents denial of sending the email is non-repudiation.
Security+ SY0-701 highlights digital signatures as a cryptographic mechanism used for authentication, integrity, and non-repudiation, especially in email security, PKI systems, and secure messaging.
Thus, the correct answer is Non-repudiation.

NEW QUESTION: 12
A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Select two).
A. Detective
B. Corrective
C. Preventive
D. Directive
E. Technical
F. Deterrent
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following is a reason why a forensic specialist would create a plan to preserve data after an modem and prioritize the sequence for performing forensic analysis?
A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold
Answer: (SHOW ANSWER)
When conducting a forensic analysis after an incident, it's essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

NEW QUESTION: 14
Several customers want an organization to verify its security controls are operating effectively and have requested an independent opinion.
Which of the following is the most efficient way to address these requests?
A. Perform an annual self-assessment.
B. Hire a vendor to perform a penetration test

C. Provide a third-party attestation report

D. Allow each client the right to audit

Answer: (SHOW ANSWER)

NEW QUESTION: 15

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	f0ddb9cbb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following in the security administrator most likely protecting against?

A. Password compromise

B. Pass-the-hash attacks

C. Account sharing

D. Weak password complexity

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of users. Which of the following would be a good use case for this task?

creating a script

A. Off-the-shelf software

B. Orchestration

C. Baseline

D. Policy enforcement

Answer: B (LEAVE A REPLY)

In the context of the CompTIA Security+ SY0-701 exam, orchestration is the most appropriate answer because it directly aligns with the automation of repetitive, operational security tasks. Orchestration refers to the coordinated execution of automated processes to streamline workflows, reduce administrative burden, and ensure consistent outcomes. Creating a script to automate user account creation for a large number of users is a textbook example of orchestration in action.

The Security+ SY0-701 study guide emphasizes that automation and orchestration are essential components of modern security operations. They are used to minimize human error, improve efficiency, and enforce consistency across environments. Manual account creation is error-prone, especially at scale, and can lead to misconfigured permissions, inconsistent group memberships, or skipped security steps. Orchestration ensures that predefined steps-such as creating user accounts, assigning roles, applying access controls, enforcing password policies, and logging actions-are executed reliably every time.

The other options do not fit the scenario. Off-the-shelf software refers to prebuilt commercial solutions rather than a custom script. A baseline defines a standard configuration state but does not automate actions. Policy enforcement ensures compliance with rules but does not perform the operational task itself. The key distinction is that orchestration focuses on execution and coordination of tasks, not governance or standards.

From a Security+ operational standpoint, orchestration supports secure identity and access management by ensuring accounts are provisioned consistently and in alignment with organizational policies. It also improves auditability and accountability by enabling predictable, repeatable processes. Therefore, orchestration is the correct and most secure solution for automating large-scale account creation.

NEW QUESTION: 17
Which of the following explains how a supply chain service provider could introduce a security vulnerability into an organization?
A. Delaying hardware shipments needed for system upgrades
B. Outsourcing customer service operations to a foreign call center
C. Failing to encrypt data stored on the organization's internal database
D. Having privileged access to client systems and becoming a target for attackers
Answer: D (LEAVE A REPLY)
The correct answer is having privileged access to client systems and becoming a target for attackers, which directly reflects a major risk discussed in the Security+ SY0-701 domain of Security Program Management and Oversight, specifically within third-party and supply chain risk management. Supply chain service providers often require elevated or privileged access to an organization's systems to perform maintenance, monitoring, software updates, or support services. This level of access significantly expands the organization' s attack surface.
When a vendor has privileged access, attackers may target the service provider as an indirect path into the primary organization. This type of compromise is especially dangerous because malicious activity may appear legitimate, using trusted credentials and authorized connections.
The Security+ study guide emphasizes that third-party compromises can bypass traditional perimeter defenses, making them particularly difficult to detect and contain. As a result, vendors can unintentionally introduce vulnerabilities even if the organization's internal security controls are strong.
The other options do not directly introduce a security vulnerability. Delayed hardware shipments affect availability and project timelines but do not create a security weakness. Outsourcing customer service may introduce privacy or compliance concerns, but it does not inherently create a technical vulnerability unless combined with poor access controls. Failing to encrypt internal databases is an internal security failure, not a supply chain issue caused by a service provider.
From a Security+ perspective, managing this risk requires strong contractual controls, least-privilege access, continuous monitoring, and audit rights. Organizations must treat vendors as extensions of their own environment. Therefore, privileged access held by a supply chain provider-and the increased likelihood of that provider being targeted-is the most accurate explanation of how a supply chain service provider can introduce a security vulnerability.

NEW QUESTION: 18
A human resources (HR) employee working from home leaves their company laptop open on the kitchen table. A family member walking through the kitchen reads an email from the Chief Financial Officer addressed to the HR department. The email contains information referencing company layoffs. The family member posts the content of the email to social media. Which of the following policies will the HR employee most likely need to review after this incident?
A. Hybrid work environment
B. Operations security
C. Data loss prevention

D. Social engineering

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:

Operations security (OPSEC) focuses on identifying and protecting sensitive information to prevent unauthorized disclosure. In this scenario, the HR employee failed to safeguard confidential company information, leading to its exposure on social media.

Training in OPSEC would reinforce the need to maintain security best practices, such as locking screens when away from a device and ensuring that sensitive data is not exposed in unsecured locations.

Hybrid work environmentpolicies relate to managing remote and in-office work but do not specifically cover security risks like unauthorized data exposure.

Data loss prevention (DLP)deals with technology-based solutions to prevent unauthorized data transfers but does not address physical security practices.

Social engineeringrefers to deceptive tactics used by attackers to manipulate individuals, which is not applicable to this situation.

The HR employee should reviewoperations securitypolicies to prevent similar incidents in the future.

NEW QUESTION: 19

Which of the following is an example of a data protection strategy that uses tokenization?

A. Encrypting databases containing sensitive data

B. Replacing sensitive data with surrogate values

C. Removing sensitive data from production systems

D. Hashing sensitive data in critical systems

Answer: B (LEAVE A REPLY)

Detailed Explanation:

Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Masking and Tokenization".

NEW QUESTION: 20

An administrator learns that users are receiving large quantities of unsolicited messages. The administrator checks the content filter and sees hundreds of messages sent to multiple users. Which of the following best describes this kind of attack?

A. Watering hole

B. Typosquatting

C. Business email compromise

D. Phishing

Answer: D (LEAVE A REPLY)

The scenario describes a large number of unsolicited emails sent to multiple users. This is characteristic of phishing, which SY0-701 defines as mass-distributed fraudulent messages designed to trick recipients into clicking malicious links, downloading malware, or divulging sensitive information.

Phishing campaigns typically involve:

High volume

Non-targeted messaging

Use of spoofed addresses or fake content

Delivery through email systems
A watering-hole attack (A) compromises a legitimate website frequented by targets-not email.
Typosquatting (B) relies on malicious websites with deceptive URLs. Business Email Compromise (C) involves highly targeted spear-phishing or impersonation attacks, not bulk email blasts.
Because this incident involves "hundreds of messages" delivered to "multiple users," it clearly matches the characteristics of a phishing attack, not a sophisticated targeted attack type.
Phishing is the most common form of social engineering and is emphasized heavily in the Security+ exam due to its frequency and effectiveness.

NEW QUESTION: 21
A program manager wants to ensure contract employees can only use the company's computers Monday through Friday from 9 a.m. to 5 p.m.
Which of the following would best enforce this access control?
A. Creating a GPO for all contract employees and setting time-of-day log-in restrictions
B. Creating a discretionary access policy and setting rule-based access for contract employees
C. Implementing an OAuth server and then setting least privilege for contract employees
D. Implementing SAML with federation to the contract employees' authentication server
Answer: A (LEAVE A REPLY)
The most appropriate method is to use aGroup Policy Object (GPO) with time-of-day restrictions (A). This is a native capability in Windows environments that allows administrators to controlwhen users are allowed to log into domain-joined systems.
This aligns withDomain 3.1: Given a scenario, apply identity and access management (IAM) concepts, especially under"Access controls (e.g., time-based restrictions, GPOs, least privilege)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.1 - "Access controls: Time-based restrictions, GPO."

NEW QUESTION: 22
Which of the following can be used to mitigate attacks from high-risk regions?
A. Obfuscation
B. Data sovereignty
C. Encryption
D. IP geolocation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
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. Develop phishing campaigns and notify the management team of any successes.
B. Evaluate tools that identify risky behavior and distribute reports on the findings.
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: C (LEAVE A REPLY)

NEW QUESTION: 24

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: B (LEAVE A REPLY)

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, andantivirus 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.

References:

Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance." CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Detective controls are designed to identify and monitor any malicious activity or anomalies on a system or network." Control Types - CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ..., under "Detective Controls":

"Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network."

NEW QUESTION: 25

Which of the following data types relates to data sovereignty?

A. Data classified as public in other countries

B. Personally Identifiable data while traveling

C. Health data shared between doctors in other nations

D. Data at rest outside of a country's borders

Answer: D (LEAVE A REPLY)

Data sovereignty concerns the laws and governance that apply to data at rest outside of a country's borders. It refers to the legal implications and regulatory controls over where data is stored geographically.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "Data sovereignty refers to data being subject to the laws of the country in which it resides." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

NEW QUESTION: 26

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: (SHOW ANSWER)

NEW QUESTION: 27
A company plans to secure its systems by:
Preventing users from sending sensitive data over corporate email
Restricting access to potentially harmful websites
Which of the following features should the company set up? (Select two).
A. Guardralls
B. Antivirus signatures
C. File integrity monitoring
D. Stateful firewall
E. DNS filtering
F. DLP software
Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 28
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: 29
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 attestationinvolveformal confirmationthat 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 toprivacy 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.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 30
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: (SHOW ANSWER)
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: 31
A company with a high-availability website is looking to harden its controls at any cost. The company wants to ensure that the site is secure by finding any possible issues. Which of the following would most likely achieve this goal?
A. Permission restrictions
B. Bug bounty program
C. Vulnerability scan
D. Reconnaissance
Answer: B (LEAVE A REPLY)
Abug bounty programencourages ethical hackers tofind and report vulnerabilities, helping organizations discover security flaws before they are exploited by malicious actors. Unlikevulnerability scans, bug bounty programs usereal-world testing techniques.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

NEW QUESTION: 32
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: 33
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:

```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

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: 34
Which security controls is a company implementing by deploying HIPS? (Select two)
A. Directive
B. Preventive
C. Physical

D. Corrective
E. Compensating
F. Detective
Answer: B,F (LEAVE A REPLY)
A Host-Based Intrusion Prevention System (HIPS) provides preventive and detective security controls.
Security+ SY0-701 explains that:
* As a preventive control (B), HIPS actively blocks malicious behavior, stops unauthorized changes, prevents exploit execution, and enforces host-level protection. It prevents malware, intrusions, and unauthorized actions before they occur.
* As a detective control (F), HIPS monitors host activity, detects suspicious patterns, logs events, and alerts administrators when threats are observed.
Directive controls (A) involve policy, not technical tools. Physical controls (C) include barriers and locks.
Corrective controls (D) restore systems after incidents. Compensating controls (E) are alternatives when primary controls aren't available.
Therefore, the correct answers are B (Preventive) and F (Detective).

NEW QUESTION: 35
Which of the following should be used to select a label for a file based on the file's value, sensitivity, or applicable regulations?
A. Verification
B. Certification
C. Classification
D. Inventory
Answer: C (LEAVE A REPLY)
Classification is the process of assigning labels to files or data based on sensitivity, business value, or regulatory requirements. Proper classification guides handling, access controls, and protection measures.
Verification (A) and certification (B) are validation processes, and inventory (D) is a listing of assets.
Data classification is a foundational data governance control in SY0-701#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 36
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: (SHOW ANSWER)
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: 37
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: 38
While considering the organization's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor.
Which of the following best meets this goal?
A. Community cloud
B. PaaS
C. Containerization
D. Private cloud
E. SaaS
F. IaaS
Answer: E (LEAVE A REPLY)
Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.
References = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

NEW QUESTION: 39
Which of the following best represents an application that does not have an on-premises requirement and is accessible from anywhere?
A. Pass
B. Hybrid cloud
C. Private cloud
D. IaaS
E. SaaS
Answer: E (LEAVE A REPLY)
Software as a Service (SaaS) represents an application that is hosted in the cloud and accessible via the internet from anywhere, with no requirement for on-premises infrastructure. SaaS applications are managed by a third-party provider, allowing users to access them through a web browser, making them highly scalable and flexible for remote access.

References:
* CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, where cloud service models such as SaaS are discussed, highlighting their accessibility and lack of on-premises requirements.

NEW QUESTION: 40
During a security incident, the security operations team identified sustained network traffic from a malicious IP address:
10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?
A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32
Answer: B (LEAVE A REPLY)
A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9
/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.
References = Firewall Rules - CompTIA Security+ SY0-401: 1.2, Firewalls - SY0-601 CompTIA Security+ :
3.3, Firewalls - CompTIA Security+ SY0-501, Understanding Firewall Rules - CompTIA Network+ N10-
005: 5.5, Configuring Windows Firewall - CompTIA A+ 220-1102 - 1.6.

NEW QUESTION: 41
A systems administrator wants to use a technical solution to explicitly define file permissions for the entire team. Which of the following should the administrator implement?
A. ACL
B. Monitoring
C. Isolation
D. HIPS
Answer: A (LEAVE A REPLY)
An Access Control List (ACL) is a technical mechanism used to explicitly define permissions for files, folders, or other resources. ACLs specify which users or system processes are granted access to objects and what operations are allowed on given objects. This allows the administrator to centrally and granularly manage file permissions for a group or team.

Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1, "Access control lists (ACLs) are used to explicitly define permissions to files and resources for users and groups." Exam Objectives 3.1: "Implement secure network architecture concepts."

NEW QUESTION: 42
A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 002.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-HT	user1
10.18.04.30	EB-AC-11-02-42-F3	PC-CA	user3
10.18.04.59	28-BB-5A-11-52-2A	PC-PA	user2
10.18.04.50	28-BB-5A-[illegible]-E9-D1	PC-TX	user4
10.18.04.22	EB-[illegible]-11-02-42-F3	WIN10	user3
10.18.04.2[illegible]	BB-28-11-21-A2-73	[illegible]-N	admin

Which of the following is the most likely way a rogue device was allowed to connect?
A. An administrator bypassed the security controls for testing.
B. A user performed a MAC cloning attack with a personal device.
C. DNS hijacking let an attacker intercept the captive portal traffic.
D. A DMCP failure caused an incorrect IP address to be distributed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
A systems administrator receives an alert that a company's internal file server is very slow and is only working intermittently. The systems administrator reviews the server management software and finds the following information about the server:

ServerName	#Connections	CPU%	MEM%	Read/s	Writes/s
FileSev01	12	99.6%	97%	50KB/s	100KB/s

Which of the following indicators most likely triggered this alert?
A. Account lockout
B. Concurrent session usage
C. Network saturation
D. Resource consumption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?
A. Unskilled attacker
B. Shadow IT
C. Credential stuffing
D. DMARC failure
Answer: A (LEAVE A REPLY)

ARP poisoning(also known as ARP spoofing) is a basicman-in-the-middle (MITM)attack that involves sending fake ARP responses to redirect traffic. This technique isnot sophisticatedand can be easily executed using freely available tools like Cain & Abel, Ettercap, or Wireshark. Such attacks are often attempted byunskilled attackers (script kiddies)testing their abilities, especially in environments like schools. The term"unskilled attacker"fits best here, as credential stuffing and DMARC are unrelated to ARP poisoning.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Attack techniques: MITM, ARP poisoning; attacker types: Unskilled/script kiddie."

NEW QUESTION: 45
Which of the following is a risk of conducting a vulnerability assessment?
A. A disruption of business operations
B. Reports of false positives
C. Unauthorized access to the system
D. Finding security gaps in the system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
A security analyst learns that an attack vector, which was used as a part of a recent incident, was a well- known IoT device exploit. The analyst needs to review logs to identify the time of initial exploit. Which of the following logs should the analyst review first?
A. Wireless access point
B. Switch
C. Firewall
D. NAC
Answer: (SHOW ANSWER)
Many IoT devices connect to the network via wireless access points. Reviewing these logs would reveal when the IoT device first connected, as well as any suspicious or anomalous traffic patterns associated with the exploit's initiation.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.1: "Wireless access point logs can help determine initial connectivity and exploitation of IoT devices." Exam Objectives 4.1: "Summarize the importance of logging and monitoring activities."

NEW QUESTION: 47
Which of the following is the best way to improve the confidentiality of remote connections to an enterprise ' s infrastructure?
A. Firewalls
B. Virtual private networks
C. Extensive logging

D. Intrusion detection systems

Answer: B (LEAVE A REPLY)

Confidentiality is primarily improved by preventing unauthorized parties from viewing data while it travels across untrusted networks. A Virtual Private Network (VPN) addresses this by creating a protected tunnel between endpoints, commonly using tunneling technologies such as IPSec or TLS for secure communications.

The Study Guide explains the purpose of VPNs for remote access as: "A virtual private network (VPN) is a way to create a virtual network link across a public network that allows the endpoints to act as though they are on the same network." It also notes the practical security value of full-tunnel VPNs when traversing untrusted networks: "A full-tunnel VPN sends all network traffic through the VPN tunnel, keeping it secure as it goes to the remote trusted network... [and] is a great way to ensure that traffic sent through an untrusted network...

remains secure."

Why the other options are less correct for confidentiality: Firewalls control traffic flow but do not inherently encrypt remote communications end-to-end; extensive logging improves detection/forensics, not confidentiality; and IDS detects suspicious activity but doesn't prevent eavesdropping on the connection. For confidentiality of remote connections, VPNs (implemented with secure tunneling like TLS/IPSec) are the best answer.

References: Sybex CompTIA Security+ Study Guide (SY0-701) - VPN definition and role ; full-tunnel VPN guidance for securing traffic over untrusted networks .

NEW QUESTION: 48

A few weeks after deploying additional email servers, a company begins to receive complaints that messages are going into recipients' spam folders. Which of the following needs to be updated?

A. CNAME

B. SMTP

C. DLP

D. SPF

Answer: D (LEAVE A REPLY)

When new email servers are deployed, organizations must update their SPF (Sender Policy Framework) records to list the new servers as authorized senders. If the SPF DNS record does not include the new IP addresses, recipient mail systems cannot verify the legitimacy of the messages, causing them to be flagged as spam or rejected.

Security+ SY0-701 identifies SPF as a key email authentication mechanism responsible for preventing:

Email spoofing

Unauthorized sender impersonation

False spam detection

Domain reputation issues

CNAME (A) maps domain aliases but does not authenticate email. SMTP (B) is the mail protocol and does not influence spam classification. DLP (C) prevents data leakage, not spam filtering.

Updating the SPF record resolves legitimacy issues by informing receiving mail servers that the new email servers are trusted.

Thus, the correct answer is D: SPF.

NEW QUESTION: 49

Which of the following techniques would identify whether data has been modified in transit?

A. Hashing

B. Tokenization

C. Masking
D. Encryption
Answer: (SHOW ANSWER)
Hashing is used to verify data integrity. By comparing the hash value of the data before and after transmission, it is possible to determine if the data has been altered in transit. If the hash values match, the data has not been modified.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3: "Hashing ensures integrity by making it possible to detect unauthorized changes to data." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 50
A company wants to minimize the chance of its outgoing marketing emails getting flagged as spam. The company decides to list the email servers on the proper DNS record. Which of the following protocols should the company apply next?
A. DMARC
B. DLP
C. DKIM
D. SPF
Answer: C (LEAVE A REPLY)
After listing authorized email servers in DNS using SPF, the next protocol the company should apply is DKIM (DomainKeys Identified Mail). DKIM provides cryptographic assurance that email messages have not been altered in transit and that they were legitimately sent by the domain owner. Security+ SY0-701 explains that DKIM works by digitally signing outgoing emails using a private key, which recipient servers verify using a public key stored in DNS.
SPF validates where an email is sent from, but it does not protect message integrity. DKIM complements SPF by ensuring the message content is authentic, which significantly improves email reputation and reduces spam filtering issues.
DMARC (A) builds on SPF and DKIM but requires both to be in place first. DLP (B) prevents data leakage and is unrelated to email reputation. SPF (D) was already applied, as stated in the question.
Thus, the correct next step is C: DKIM.

NEW QUESTION: 51
An accounting employee recently used software that was not approved by the company. Which of the following risks does this most likely represent?
A. Unskilled attacker
B. Hacktivist
C. Shadow IT
D. Supply chain
Answer: C (LEAVE A REPLY)
Shadow IT refers to employees using software or services without official approval, often introducing security risks due to lack of control, monitoring, or compliance. This can lead to vulnerabilities, data leakage, or policy violations.
Unskilled attacker (A) and hacktivist (B) are threat actor types; supply chain (D) refers to risks from external partners or vendors, not internal unauthorized software usage.
Shadow IT is highlighted in Security Program Management and Threats domains for its risk implications#6:
Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 52
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: 53
Which of the following would be thebestway to block unknown programs from executing?
A. Access control list
B. Application allow list.
C. Host-based firewall
D. DLP solution
Answer: B (LEAVE A REPLY)
An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network12.
The other options are not the best ways to block unknown programs from executing:
Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control thepermissions and privileges of users or groups, but it does not directly block unknown programs from executing13.
Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing1 .

DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing1 .
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting
- CompTIA Security+ SY0-701 - 3.5, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. :
CompTIA Security+ SY0-701 Certification Study Guide, page 100.

NEW QUESTION: 54
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: A (LEAVE A REPLY)
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: 55
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 streamlineaccount 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 thecommunication, 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: 56
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: 57
A network administrator deploys an FDE solution on all end user workstations. Which of the following data protection strategies does this describe?
A. Masking
B. Data in transit
C. Obfuscation
D. Data at rest
E. Data sovereignty
Answer: (SHOW ANSWER)
Full-disk encryption (FDE) protects the contents of storage media, which is a classic data-at-rest control. The Study Guide explains the "three situations" relevant to confidentiality-at rest, in transit, and in use-and then specifically ties disk encryption/FDE to protecting stored data: "Data at rest, or stored data, is that which resides in a permanent location awaiting access... Examples... hard drives..." It then describes FDE as an encryption method applied to disks: "Full-disk encryption (FDE) is a form of encryption where all the data on a hard drive is automatically encrypted, including the operating system and system files... In the case of loss or theft, FDE can prevent unauthorized access to all data on the hard drive." That is exactly the definition of protecting data at rest-it is intended to prevent disclosure if a laptop /workstation is lost, stolen, or the drive is removed. This is not masking (hiding parts of fields), not data in transit (network encryption like TLS/VPN), not obfuscation (making code hard to understand), and not data sovereignty (jurisdiction/location requirements). Therefore, deploying FDE on workstations is a data-at-rest protection strategy.

References: Data-at-rest definition and confidentiality contexts ; FDE definition and purpose protecting disk- stored data .

NEW QUESTION: 58
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: 59
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	f8ddb9cbb321d7dfbf6cb059736f0b3d
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: C (LEAVE A REPLY)
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: 60
A security engineer is installing an IPS to block signature-based attacks in the environment. Which of the following modes will best accomplish this task?

A. Monitor
B. Sensor
C. Audit
D. Active
Answer: D (LEAVE A REPLY)
To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network.
Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic without actively blocking it.
Audit mode is used for review purposes and does not actively block traffic.

NEW QUESTION: 61
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: D (LEAVE A REPLY)
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3:
Technologies and Tools, page 1222.

NEW QUESTION: 62
Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?
A. Degaussing
B. Formatting
C. Sanitization

D. Defragmentation
Answer: (SHOW ANSWER)

NEW QUESTION: 63
A security administrator protects passwords by using hashing. Which of the following best describes what the administrator is doing?
A. Adding extra characters at the end to increase password length
B. Generating a token to make the passwords temporal
C. Using mathematical algorithms to make passwords unique
D. Creating a rainbow table to protect passwords in a list
Answer: (SHOW ANSWER)
Hashing is the process of converting plaintext passwords into a fixed-length, irreversible string using a mathematical algorithm (hash function). This makes each password unique based on its content, and even a small change in the password will produce a different hash. The primary purpose is to ensure that the actual passwords are not stored directly and cannot be easily recovered from the hash, even if the hash is compromised.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Hashing ensures that plaintext passwords are not stored directly. Hash functions use mathematical algorithms to produce unique, fixed-length output for each unique input." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 64
A security analyst is assessing several company firewalls. Which of the following cools would The analyst most likely use to generate custom packets to use during the assessment?
A. hping
B. Wireshark
C. PowerShell
D. netstat
Answer: (SHOW ANSWER)
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: 65
Which of the following should a security team do first before a new web server goes live?
A. Harden the virtual host.
B. Create WAF rules.
C. Enable network intrusion detection.
D. Apply patch management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
A security analyst estimates that a small security incident will cost $10,000 and will occur twice per year. The analyst recommends a budget of $20,000 for next year. Which of the following does the $10,000 represent?
A. ARO
B. SLE
C. ALE
D. RPO
Answer: (SHOW ANSWER)
The $10,000 is the estimated cost per incident (per single occurrence). In quantitative risk analysis, that value is the Single Loss Expectancy (SLE)-the financial impact expected each time a risk event occurs. The Study Guide defines these terms and calculations clearly: "The single loss expectancy (SLE) is the amount of financial damage expected each time a risk materializes." It also explains how annual impact is derived: "The annualized loss expectancy (ALE) is the amount of damage expected from a risk each year. It is calculated by multiplying the SLE and the ARO." Here, the event occurs twice per year, so the Annualized Rate of Occurrence (ARO) is 2.0, and the annual expected loss (ALE) would be SLE × ARO = $10,000 × 2 = $20,000, which matches the recommended budget. That confirms $10,000 is not ARO (a frequency), not ALE (annual total), and not RPO (a disaster recovery metric about acceptable data loss window).
References: Quantitative risk terms and formulas (SLE definition; ALE = SLE × ARO) .

NEW QUESTION: 67
Which of the following best describes a method for ongoing vendor monitoring in third-party risk management?
A. Requiring a new MSA for each project
B. Accepting vendor self-attestation without further verification
C. Conducting assessments to verify compliance with security requirements
D. Reviewing SLAs at the start of the contract
Answer: (SHOW ANSWER)
Ongoing vendor monitoring is a critical component of third-party risk management (TPRM) and focuses on continuously validating that vendors maintain required security controls throughout the lifecycle of the relationship. According to CompTIA Security+ SY0-701, the most effective ongoing monitoring method is conducting assessments to verify compliance with security requirements. These assessments may include periodic security questionnaires, audits, penetration test results, SOC reports, or compliance attestations that are independently validated.
Option A, requiring a new MSA for each project, is a contractual activity, not a monitoring mechanism.
Option B-accepting self-attestation without verification-introduces risk and is specifically discouraged in SY0-701 because it lacks assurance.
Option D, reviewing SLAs at contract start, is a one-time activity and does not provide continuous oversight.
Ongoing assessments allow organizations to detect control drift, identify new risks, and ensure vendors remain compliant with evolving regulatory and security expectations. This proactive approach is essential for managing supply chain risk and protecting organizational data.
Therefore, the correct answer is C: Conducting assessments to verify compliance with security requirements.

NEW QUESTION: 68
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: 69
Which of the following tasks is typically included in the BIA process?
A. Establishing the backup and recovery procedures
B. Identifying the communication strategy
C. Estimating the recovery time of systems
D. Developing the incident response plan
E. Evaluating the risk management plan
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following could potentially be introduced at the time of side loading?
A. User impersonation
B. Rootkit
C. On-path attack
D. Buffer overflow
Answer: B (LEAVE A REPLY)
Side loading is the process of installing applications from unofficial sources, often bypassing standard app stores. This increases the risk of installing malicious software, such as a rootkit, which is a type of malware designed to provide persistent privileged access while hiding its presence.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Side loading applications from unofficial sources can introduce malware, such as rootkits, to the system." Exam Objectives 2.1: "Compare and contrast different types of threats."

NEW QUESTION: 71

A store is setting up wireless access for employees. Management wants to limit the number of access points while ensuring full coverage. Which tool will help determine how many access points are needed?

A. Signal locator

B. WPA3

C. Heat map

D. Site survey

Answer: D (LEAVE A REPLY)

A site survey is the formal process used to determine the required number, placement, and configuration of wireless access points (APs). Security+ SY0-701 states that site surveys measure RF propagation, identify dead zones, account for building materials, detect interference sources, and evaluate coverage overlap. This information allows network engineers to deploy the fewest APs necessary while still ensuring full coverage.

Although heat maps (C) are generated as a result of a site survey, they are visualization tools-not the actual survey process. A signal locator (A) is not a standardized tool in wireless planning. WPA3 (B) is a wireless security protocol and has no impact on access point planning or coverage optimization.

A full site survey ensures optimal AP placement to balance coverage, performance, and cost-exactly the concern described in the scenario. Thus, the correct answer is D: Site survey.

NEW QUESTION: 72

Which of the following would a security administrator use to comply with a secure baseline during a patch update?

A. Information security policy

B. Service-level expectations

C. Standard operating procedure

D. Test result report

Answer: (SHOW ANSWER)

Detailed Explanation:Standard operating procedures (SOPs) outline the steps to be followed to maintain a secure baseline, such as testing and deploying patches while minimizing risk to the system. Reference:

CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Patch Management and Baseline Compliance".

NEW QUESTION: 73

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: 74
A vendor salesperson is a personal friend of a company's Chief Financial Officer (CFO). The company recently made a large purchase from the vendor, which was directly approved by the CFO. Which of the following best describes this situation?
A. Rules of engagement
B. Conflict of interest
C. Due diligence
D. Contractual impact
E. Reputational damage
Answer: B (LEAVE A REPLY)
Aconflict of interest (B)arises when personal relationships or interests could potentially influence professional decisions. In this case, the CFO's friendship with the vendor could improperly affect the procurement decision- making process.
This scenario falls underDomain 5.3: Explain the importance of frameworks, policies, procedures, and controls-specifically under"Personnel policies (e.g., conflict of interest, mandatory vacations, job rotation)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.3 - "Personnel policies: Conflict of interest."

NEW QUESTION: 75
Which of the following best describe why a process would require a two-person integrity security control?
A. To Increase the chance that the activity will be completed in half of the time the process would take only one user to complete
B. To permit two users from another department to observe the activity that is being performed by an authorized user
C. To reduce the risk that the procedures are performed incorrectly or by an unauthorized user
D. To allow one person to perform the activity while being recorded on the CCTV camera
Answer: (SHOW ANSWER)
A two-person integrity security control is implemented to minimize the risk of errors or unauthorized actions.
This control ensures that at least two individuals are involved in critical operations, which helps to verify the accuracy of the process and prevents unauthorized users from acting alone. It's a security measure commonly used in sensitive operations, like financial transactions or access to critical systems, to ensure accountability and accuracy.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Security Operations and Management.

NEW QUESTION: 76
An organization wants to donate its aging network hardware. Which of the following should the organization perform to prevent any network details from leaking?
A. Destruction
B. Sanitization
C. Certification
D. Data retention
Answer: B (LEAVE A REPLY)
Sanitization is the process of thoroughly removing or wiping all data from devices before disposal or donation to prevent sensitive information from being recovered or leaked.
Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 4.4: "Sanitization is used to ensure data cannot be recovered from donated or decommissioned equipment." Exam Objectives 4.4: "Summarize business continuity and disaster recovery concepts."

NEW QUESTION: 77
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: 78
Which of the following would most likely prevent exploitation of an end-of-life, business-critical system?
A. Monitoring
B. Isolation
C. Decommissioning
D. Encryption
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
End-of-life (EOL) systems no longer receive security patches, vendor support, or vulnerability updates.
Because of this, they are highly susceptible to exploitation, especially if attackers can reach them over a network. When the system is business-critical and cannot be decommissioned, the most effective strategy is isolation, also known as network segmentation, air-gapping, or restrictive network zoning. Isolation removes direct exposure to external and internal threats by limiting communication paths to only essential systems and users.
According to the Security+ SY0-701 guidance, isolating legacy systems helps reduce the attack surface when patching is no longer possible.
Monitoring (A) is useful for detection but does not prevent exploitation.

Decommissioning (C) would be ideal but is not possible for business-critical systems, as stated in the question. Encryption (D) protects data confidentiality but does not stop an attacker from exploiting vulnerabilities in an unpatched OS or application.
Isolation is a recommended compensating control for legacy and unsupported systems in SY0-701's Security Architecture & Resilience domain, which emphasizes micro-segmentation, firewalls, and restricted access to minimize risk when systems cannot be replaced or patched.

NEW QUESTION: 79
A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.
Which of the following best describes the program the company is setting up?
A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing
Answer: B (LEAVE A REPLY)
A bug bounty is a program that rewards security researchers for finding and reporting vulnerabilities in an application or system. Bug bounties are often used by companies to improve their security posture and incentivize ethical hacking. A bug bounty program typically defines the scope, rules, and compensation for the researchers. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 10. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.

NEW QUESTION: 80
A new corporate policy requires all staff to use multifactor authentication to access company resources.
Which of the following can be utilized to set up this form of identity and access management? (Select two)
A. Authentication tokens
B. Least privilege
C. Biometrics
D. LDAP
E. Password vaulting
F. SAML
Answer: A,C (LEAVE A REPLY)
Multifactor authentication (MFA) requires users to provide two or more of the following categories:
Something you know (password/PIN)
Something you have (token/smart card)
Something you are (biometrics)
Authentication tokens (A) qualify as something you have, such as hardware tokens, OTP apps, or smart cards.
Biometrics (C) qualify as something you are, such as fingerprint scans, facial recognition, or iris scans. Using these two together easily establishes MFA.
Least privilege (B) is an authorization principle, not an MFA factor. LDAP (D) is a directory service protocol, not an MFA mechanism. Password vaulting (E) assists with credential storage but does not implement MFA.
SAML (F) is a federation protocol used for Single Sign-On (SSO), not inherently MFA.
Thus, the correct MFA components are A: Authentication tokens and C: Biometrics.

NEW QUESTION: 81
A security administrator is implementing encryption on all hard drives in an organization. Which of the following security concepts is the administrator applying?
A. Integrity
B. Authentication
C. Zero Trust
D. Confidentiality
Answer: D (LEAVE A REPLY)
Encrypting hard drives is a direct implementation of confidentiality, one of the three pillars of the CIA Triad emphasized in CompTIA Security+ SY0-701. Full disk encryption ensures that if a laptop, workstation, or server drive is stolen or accessed without authorization, the data remains unreadable without the decryption key.
This controls unauthorized disclosure and protects sensitive business, financial, and personal information.
Drive encryption is widely required for compliance frameworks such as HIPAA, PCI-DSS, and GDPR.
Integrity (A) refers to preventing unauthorized modification of data, which encryption alone does not guarantee. Authentication (B) confirms user identity, such as passwords or biometrics, but is unrelated to data- at-rest protection. Zero Trust (C) is an architectural model requiring constant verification; it is not a control for hard drive encryption.
Since the sole purpose of encrypting storage is to ensure data confidentiality, the correct answer is D.

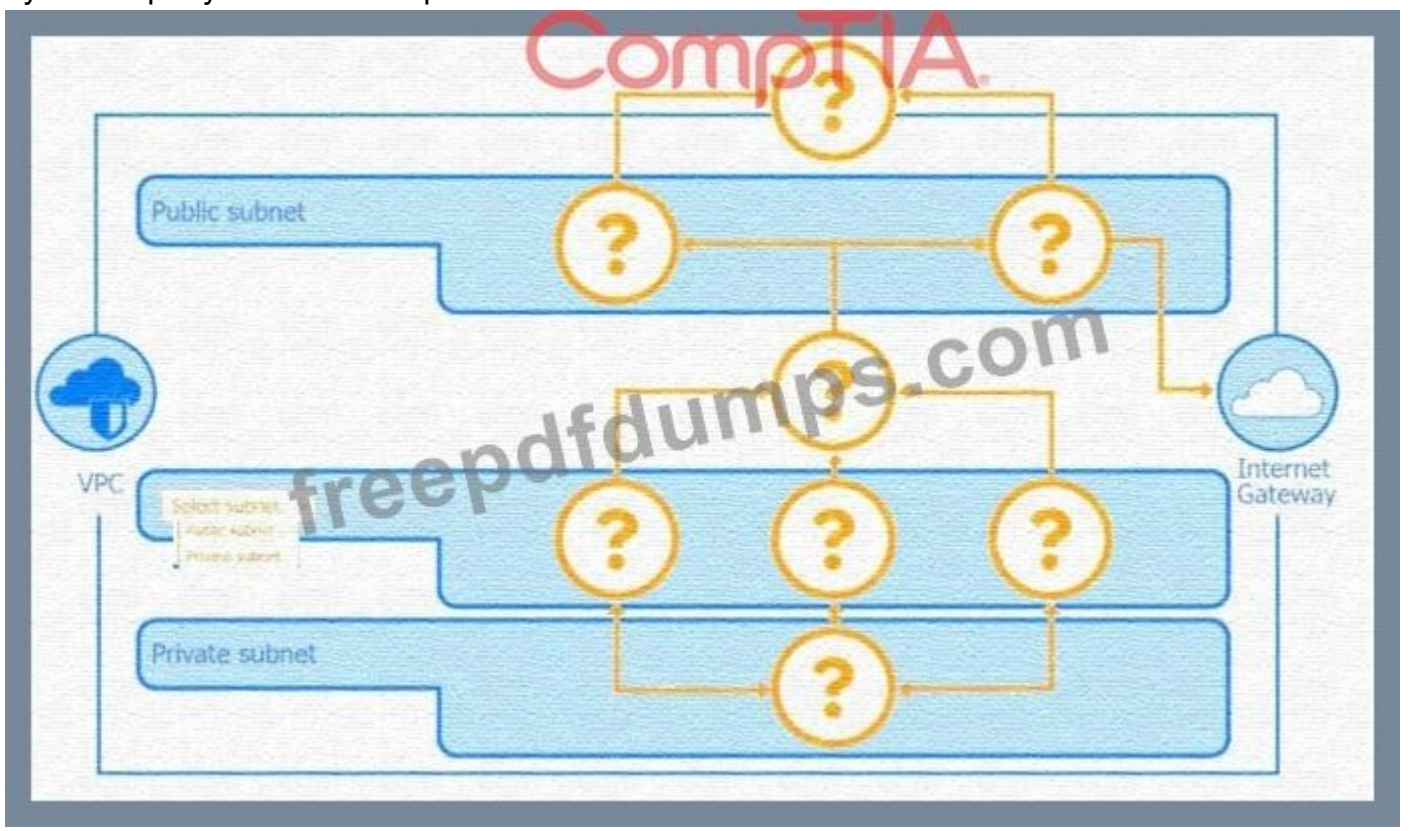
NEW QUESTION: 82
Which of the following actions would reduce the number of false positives for an analyst to manually review?
A. Create playbooks as part of a SOAR platform
B. Redefine the patch management process
C. Replace an EDR tool with an XDR solution
D. Disable AV heuristics scanning
Answer: A (LEAVE A REPLY)
Implementing playbooks as part of a SOAR (Security Orchestration, Automation, and Response) platform enables the automation of routine security tasks and the standardized response to common alerts. Playbooks help filter and validate alerts, reducing the number of false positives that analysts need to manually investigate. SOAR tools are specifically designed to improve efficiency, consistency, and accuracy in incident response, allowing analysts to focus on genuine threats rather than being overwhelmed by noise.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.3: "SOAR platforms allow organizations to automate repetitive security tasks, including the use of playbooks, to reduce false positives and the workload on analysts." Exam Objectives 4.3: "Implement incident response and recovery procedures."

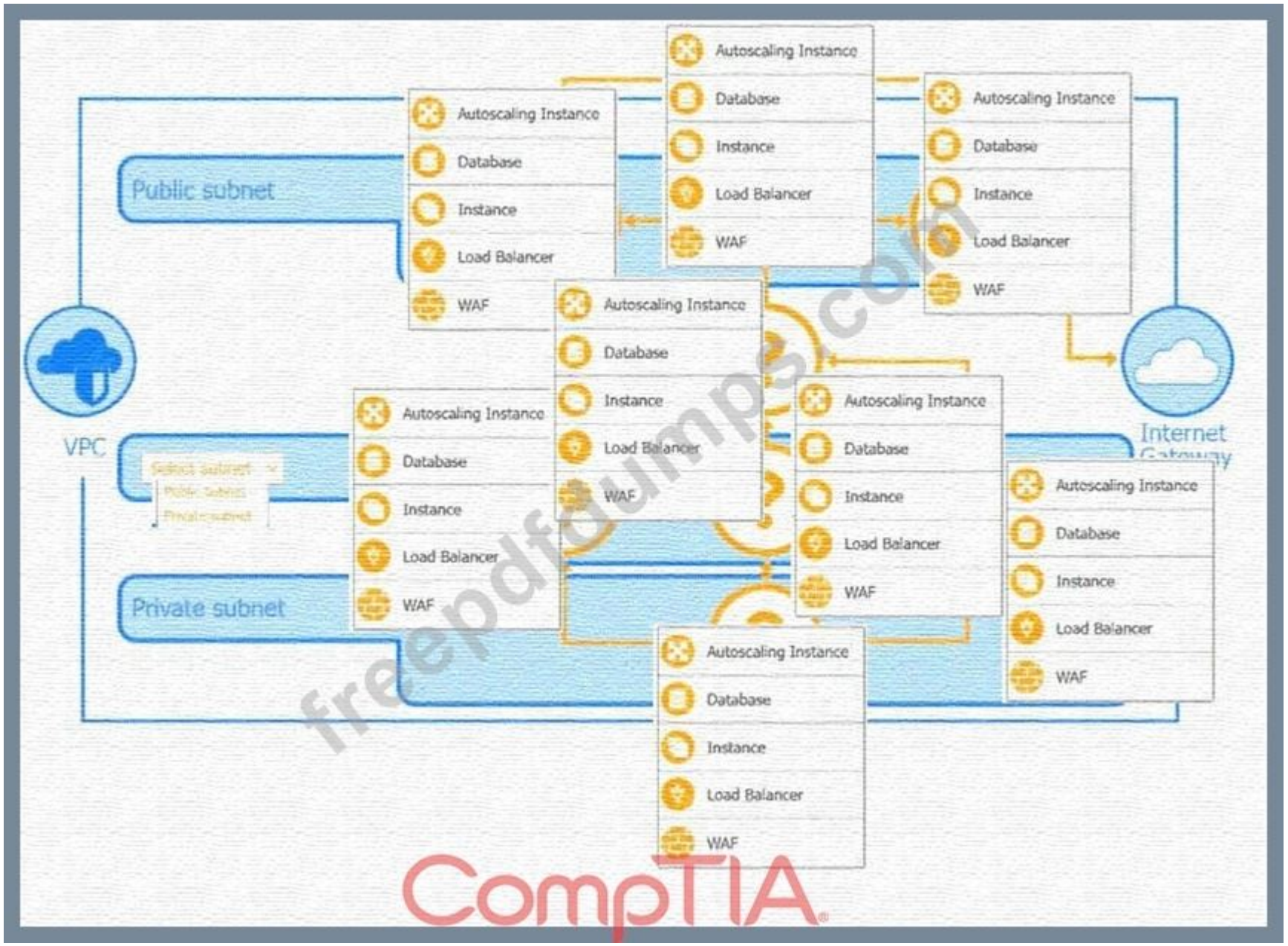
NEW QUESTION: 83
Which of the following activities should a systems administrator perform to quarantine a potentially infected system?
A. Move the device into an air-gapped environment.
B. Disable remote log-in through Group Policy.
C. Convert the device into a sandbox.
D. Remote wipe the device using the MDM platform.
Answer: A (LEAVE A REPLY)

Detailed Explanation:Quarantining a potentially infected system by placing it into an air-gapped environment physically disconnects it from the network. This prevents the spread of malware while maintaining the integrity of forensic evidence. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Incident Response and Containment".

NEW QUESTION: 84
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: B (LEAVE A REPLY)
AMaster Service Agreement (MSA)establishesthe general terms and conditionsfor ongoing business engagements. This allows companies toreuse the same termsacross 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 onservice performance expectations, not overall contract terms.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 85
A security analyst is creating the first draft of a network diagram for the company's new customer-facing payment application that will be hosted by a third-party cloud service provider.



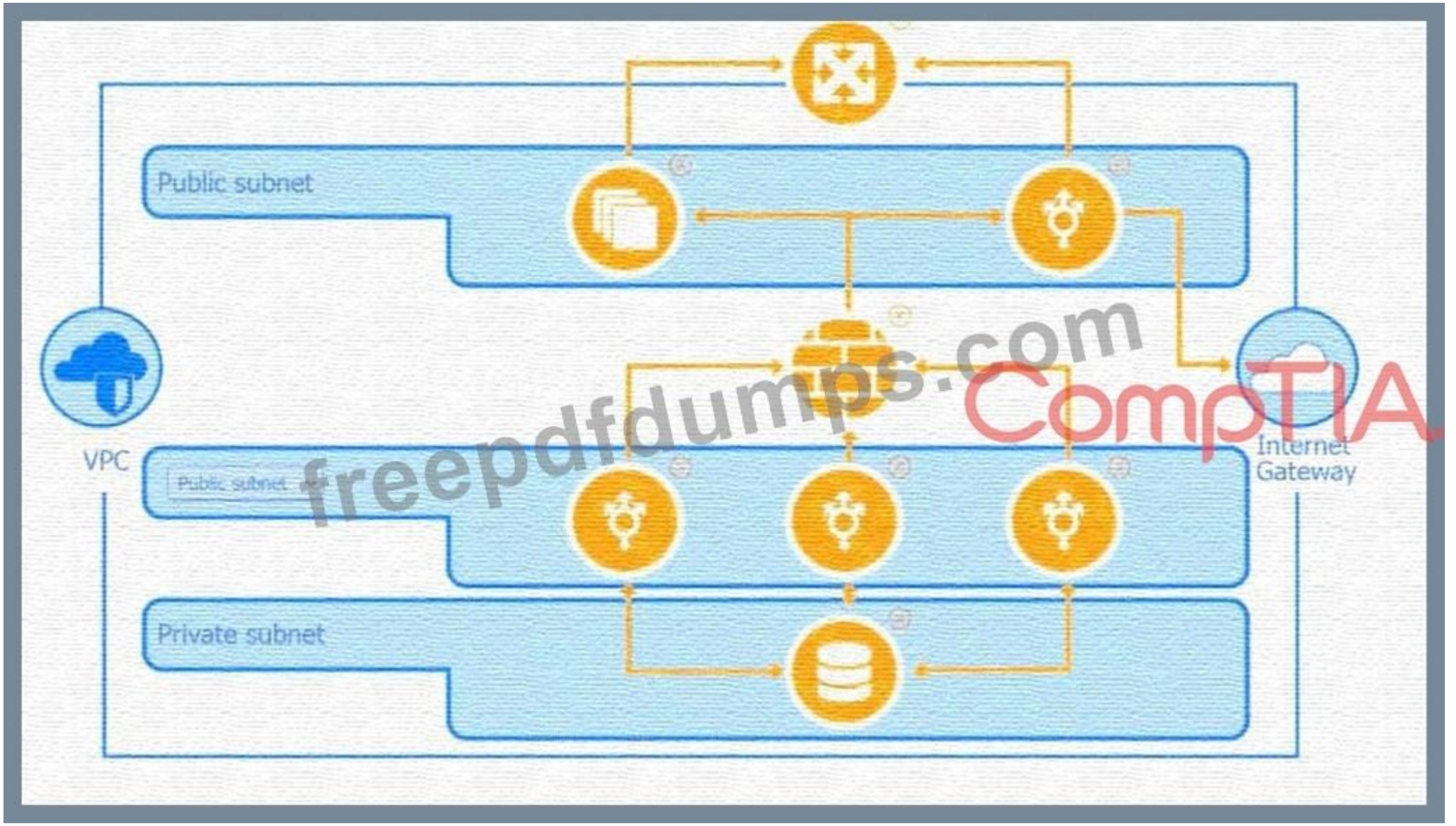


Answer:

See the Explanation for complete solution for this task.

Explanation:

A diagram of a computer AI-generated content may be incorrect.



Step 1: Understand Requirements & Security Principles

Requirements:

Customer-facing payment application (PCI DSS compliance applies)

Hosted on third-party cloud (e.g., AWS)

Must segment public-facing and internal resources

Needs to be scalable and resilient

Must have strong security controls

Step 2: Design the High-Level Network Layout

Core Components:

VPC (Virtual Private Cloud): Isolates your environment from other tenants in the cloud.

Subnets:

Public subnet: For resources that must communicate with the internet.

Private subnet: For internal resources, NOT directly exposed to the internet.

Step 3: Place Resources in Appropriate Subnets

Public Subnet:

Internet-facing Load Balancer (LB): Distributes traffic to application servers.

Web Application Firewall (WAF): Protects against web exploits.
Autoscaling Instances: EC2 (or VM) servers running your web front-end, automatically scaling as traffic grows.
Private Subnet:
Application servers: Back-end logic, not exposed to internet directly.
Database: Sensitive data storage, only accessible by application servers.
Internal Load Balancer: Manages traffic among app servers.
WAF: Can be used internally as well for defense-in-depth.
Step 4: Add Connectivity and Security Controls
Internet Gateway: Allows resources in public subnet to communicate with the internet.
NAT Gateway: Allows outbound internet traffic from private subnet without exposing private IPs.
Security Groups: Firewalls at the instance level; allow only necessary traffic (e.g., LB to web server, web server to DB).
Network ACLs: Subnet-level firewalls for additional control.
Step 5: Network Diagram Explanation (Based on Your Images)
Public Subnet (Top Layer)
Load Balancer
Accepts HTTPS traffic from customers.
Sends only necessary HTTP/HTTPS to web servers in public subnet.
WAF (Web Application Firewall)
Sits in front of Load Balancer.
Filters malicious requests (SQLi, XSS, etc.).
Autoscaling Group
Multiple web servers for redundancy and scalability.
Placed in public subnet to respond to traffic spikes.
Private Subnet (Bottom Layer)
Application Servers
Receive requests from public subnet's load balancer.
Not directly exposed to the internet.
Database
Only accessible from application servers, never public.
Security groups restrict all inbound traffic except from app servers.
Internal Load Balancer
Balances requests to application servers.
Step 6: Flow of Data (Step-by-Step)
Client -> Internet Gateway -> WAF -> Load Balancer (Public Subnet):Customers initiate connections to your app over the internet.
Load Balancer -> Autoscaling Web Servers (Public Subnet):Load balancer routes requests to available web servers.
Web Servers -> Application Logic (Private Subnet):Web servers pass necessary requests to the internal application servers.
App Servers -> Database (Private Subnet):Application servers query/update customer payment data in the database.
Outbound (NAT Gateway):App servers may need to access updates or external APIs-use NAT Gateway for secure outbound connections.
Step 7: Security Best Practices
Security Groups: Only allow necessary ports (e.g., 443 for HTTPS to LB, 3306 for MySQL between app server and DB).
Network ACLs: Add another layer of subnet-level restrictions.

Encryption: Use HTTPS for all external connections, encrypt data at rest and in transit (TLS, disk encryption).
IAM Roles/Policies: Principle of least privilege for accessing resources.
Monitoring/Logging: Enable VPC flow logs, cloud service logs, and application logging.
Patch Management: Automate patching for OS and applications.
Backups: Regular, secure backups of critical data.
Step 8: Compliance Considerations
For payment applications (PCI DSS):
Isolate cardholder data environment (CDE).
Strong access controls (multi-factor authentication, role separation).
Regular vulnerability assessments and penetration testing.
Retain logs for auditing.
Step 9: Draw the Architecture (Summary)
Internet Gateway: Allows inbound/outbound internet access.
Public Subnet: WAF, Load Balancer, Autoscaling group.
Private Subnet: App servers, DB, internal LB.
NAT Gateway: Outbound access for private resources.
Security Groups/ACLs: Control all traffic flows.
Monitoring/Logging: Enabled at all levels.
Bonus: Sample Security Group Rules
Web Server (Public Subnet):
Inbound: 443 (HTTPS) from Internet
Outbound: 80/443 to App Servers
App Server (Private Subnet):
Inbound: 80/443 from Web Servers
Outbound: 3306 (MySQL) to Database
Database (Private Subnet):
Inbound: 3306 from App Servers
Outbound: None (unless replication required)
References to Security+ Domains
1.0 General Security Concepts: Principle of least privilege, defense in depth.
2.0 Threats, Vulnerabilities, Mitigations: WAF, segmentation, patching.
3.0 Security Architecture: Network segmentation, secure design.
4.0 Security Operations: Monitoring, logging, response.
5.0 Security Program Management: Compliance, policy.

NEW QUESTION: 86
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: A (LEAVE A REPLY)
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: 87
A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?
A. Place posters around the office to raise awareness of common phishing activities.
B. Implement email security filters to prevent phishing emails from being delivered
C. Update the EDR policies to block automatic execution of downloaded programs.
D. Create additional training for users to recognize the signs of phishing attempts.
Answer: C (LEAVE A REPLY)
An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.
The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email.
Therefore, these options are not the best answer for this question. References = Endpoint Detection and Response - CompTIA Security+ SY0-701 - 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

NEW QUESTION: 88
During a routine audit, an analyst discovers that a department at a high school uses a simulation program that was not properly vetted before deployment.
Which of the following threats is this an example of?
A. Zero-day
B. C
C. Shadow IT
D. Data exfiltration
E. Espionage

Answer: (SHOW ANSWER)

NEW QUESTION: 89
A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?
A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege
Answer: D (LEAVE A REPLY)
The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-
701, 9th Edition, page 931

NEW QUESTION: 90
A new employee accessed an unauthorized website. An investigation found that the employee violated the company's rules. Which of the following did the employee violate?
A. MOU
B. AUP
C. NDA
D. MOA
Answer: B (LEAVE A REPLY)
An Acceptable Use Policy (AUP) defines what users are permitted and prohibited from doing on an organization's systems, including website access. Accessing unauthorized sites is a common violation of the AUP.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "AUPs outline what is and is not acceptable use of organizational resources."
Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks."

NEW QUESTION: 91
Executives at a company are concerned about employees accessing systems and information about sensitive company projects unrelated to the employees' normal job duties. Which of the following enterprise security capabilities will the security team most likely deploy to detect that activity?
A. UBA
B. DLP
C. NAC
D. EDR
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
During a penetration test in a hypervisor, the security engineer is able to use a script to inject a malicious payload and access the host filesystem. Which of the following best describes this vulnerability?
A. VM escape
B. Cross-site scripting
C. Malicious update
D. SQL injection
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
VM escape occurs when an attacker inside a virtual machine breaks out of the guest OS and gains access to the underlying host hypervisor or other virtual machines. In this scenario, the penetration tester executes a script to inject a malicious payload that allows access to the host filesystem-this is the textbook definition of VM escape.
The SY0-701 exam specifically identifies VM escape as one of the most critical virtualization vulnerabilities, as it defeats isolation and can compromise entire virtual environments. This typically results from flaws in hypervisor software, improper sandboxing, or insecure VM tools.
Cross-site scripting (B) affects web applications and browsers, not hypervisors. Malicious updates (C) involve tampered patch delivery. SQL injection (D) targets databases through application input fields.
Because the attacker moved from a VM to the host system, the correct classification is VM escape, a high- severity virtualization vulnerability.

NEW QUESTION: 93
An organization designs an inbound firewall with a fail-open configuration while implementing a website.
Which of the following does the organization consider to be the highest priority?
A. Confidentiality
B. Non-repudiation
C. Availability
D. Integrity
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A fail-open configuration means that if the firewall experiences an outage or failure, traffic is allowed to pass through rather than being blocked. This design decision directly prioritizes availability over other security principles.
The CIA Triad (Confidentiality, Integrity, Availability) is central in SY0-701. A fail-open firewall risks allowing unauthorized or malicious traffic during a failure, sacrificing security controls in order to maintain service uptime. This is typically used in environments where interruptions are unacceptable, such as:
Public-facing websites
Critical customer applications

Healthcare systems
Financial transaction portals
Fail-closed configurations, in contrast, prioritize confidentiality and integrity by blocking traffic when a failure occurs.
Because the organization chose fail-open, it demonstrates that maintaining continuous access to the website is more important than preventing potential exposure. This approach is aligned with the Availability pillar of the CIA model.
The SY0-701 exam emphasizes this design choice under General Security Concepts, specifically in resilience, failover mechanisms, and risk-based decisions when selecting fail-open vs. fail-closed strategies.

NEW QUESTION: 94
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. Government sanctions
B. Non-compliance
C. Rules of engagement
D. Contract violations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
A security consultant is working with a client that wants to physically isolate its secure systems. Which of the following best describes this architecture?
A. Air gapped
B. SDN
C. Highly available
D. Containerized
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
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: 97
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: 98
A security analyst sees an increase of vulnerabilities on workstations after a deployment of a company group policy. Which of the following vulnerability types will the analyst most likely find on the workstations?
A. Misconfiguration
B. Zero-day
C. Malicious update
D. Supply chain
Answer: (SHOW ANSWER)
Group policies can inadvertently introduce misconfigurations, such as enabling insecure settings or failing to disable legacy protocols, increasing vulnerabilities.
Zero-day (B) are previously unknown vulnerabilities, malicious updates (C) are attacker-controlled, and supply chain (D) risks come from third-party components.
Misconfiguration vulnerabilities are commonly introduced during changes and are emphasized in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 99
A security team installs an IPS on an organization's network and needs to configure the system to detect and prevent specific network attacks. Which of the following settings should the team configure first within the IPS?
A. Allow list policies
B. Packet Inspection
C. Logging and reporting
D. Firewall rules
Answer: (SHOW ANSWER)
An Intrusion Prevention System (IPS) uses packet inspection (either signature-based, anomaly-based, or both) to analyze network traffic and detect malicious patterns. Configuring packet inspection is the first step to ensure the IPS can identify and respond to specific attack signatures.
Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "IPS devices must be configured to inspect network packets for attack patterns."
Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

NEW QUESTION: 100
Which of the following technologies must be used in an organization that intends to automate infrastructure deployment?
A. IaC
B. IaaS
C. IoC
D. IoT
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Infrastructure as Code (IaC) is the technology required for automating infrastructure deployment. IaC allows organizations to define and deploy servers, networks, containers, and cloud resources using machine-readable configuration files rather than manual configuration. This leads to faster deployment, consistent environments, repeatability, version control, and lower human error.
CompTIA Security+ SY0-701 highlights IaC as a foundational component of DevOps and modern cloud operations. It supports automated provisioning through tools such as Terraform, Ansible, CloudFormation, and Puppet. IaC also enhances security by enabling automated compliance checks and standardized hardened configurations.
IaaS (B) is a cloud service model, not an automation mechanism. IoC (C) refers to Indicators of Compromise used in threat intelligence. IoT (D) refers to Internet-connected devices and is unrelated to infrastructure deployment.
Therefore, IaC is the required technology for automated, repeatable, secure infrastructure deployments.

NEW QUESTION: 101
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 apenetration 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: 102
Which of the following digital forensics activities would a security team perform when responding to legal requests in a pending investigation?
A. E-discovery
B. User provisioning

C. Firewall log export
D. Root cause analysis
Answer: A (LEAVE A REPLY)
E-discovery (electronic discovery) is the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or investigation. It is a critical component of digital forensics when dealing with litigation, compliance, or regulatory matters.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.5: "E-discovery is performed to identify and produce digital evidence in legal investigations." Exam Objectives 4.5: "Summarize digital forensics concepts."

NEW QUESTION: 103
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 thebestresponses 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: 104
A penetration tester visits a client's website and downloads the site's content. Which of the following actions is the penetration tester performing?
A. Unknown environment testing
B. Vulnerability scan
C. Due diligence
D. Passive reconnaissance
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
The described activity-visiting a website and downloading publicly accessible content-is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.
According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:
Public websites
DNS records

News articles
Metadata
Public document repositories
The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic. Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning. Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.
Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

NEW QUESTION: 105
Which of the following is the most likely motivation for a hacktivist?
A. Financial gain
B. Service disruption
C. Philosophical beliefs
D. Corporate espionage
Answer: C (LEAVE A REPLY)
Hacktivists are individuals or groups who use hacking to promote a political agenda, social cause, or philosophical beliefs. Their primary motivation is not personal gain but rather to draw attention to, or protest against, perceived injustices or causes.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Hacktivists are motivated by ideology or political/social causes." Exam Objectives 2.1: "Compare and contrast different types of threat actors."

NEW QUESTION: 106
Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?
A. Physical
B. Managerial
C. Technical
D. Operational
Answer: A (LEAVE A REPLY)
A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors. Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

NEW QUESTION: 107
Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?
A. ARO
B. RTO
C. RPO
D. ALE
E. SLE
Answer: D (LEAVE A REPLY)
The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions.References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 108
A government official receives a blank envelope containing photos and a note instructing the official to wire a large sum of money by midnight to prevent the photos from being leaked on the Internet. Which of the following best describes the threat actor's intent?
A. Organized crime
B. Philosophical beliefs
C. Espionage
D. Blackmail
Answer: D (LEAVE A REPLY)
The threat actor's intent is clearly blackmail, a form of extortion where sensitive information is used to coerce an individual into taking an action, usually involving financial gain. In this scenario, the attacker threatens to leak incriminating or compromising photos unless the government official wires a large sum of money.
CompTIA Security+ SY0-701 defines blackmail as the use of sensitive or embarrassing information to manipulate or force actions from victims. This differs from organized crime (A), which focuses on profit-driven cyber operations but typically uses technical attacks such as ransomware, data theft, or fraud rather than anonymous mailed threats. Philosophical beliefs (B) refers to hacktivism, where attackers pursue ideological motives-not present here. Espionage (C) involves intelligence gathering for political or competitive advantage, typically performed by nation-states or advanced persistent threats (APTs).
This scenario aligns directly with extortion-based social engineering, where attackers manipulate victims through fear and emotional pressure. According to Security+ guidance, blackmail often occurs through email, physical mail, or compromised personal data leaks, all fitting this situation. Therefore, the threat actor's intent is blackmail.

NEW QUESTION: 109

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: (SHOW ANSWER)

Cloud-based models provide strong security with features like encryption, redundancy, and disaster recovery, making it a secure choice for international operations.

NEW QUESTION: 110

An unexpected and out-of-character email message from a Chief Executive Officer's corporate account asked an employee to provide financial information and to change the recipient's contact number. Which of the following attack vectors is most likely being used?

A. Business email compromise

B. Phishing

C. Brand impersonation

D. Pretexting

Answer: A (LEAVE A REPLY)

Business Email Compromise (BEC)is atargeted phishing attackin whichattackers impersonate executives or high-ranking officials(such as a CEO) to manipulate employees intotransferring money or providing sensitive data. Since the request is coming from the CEO's corporate email (possibly spoofed or compromised), this is aclassic example of BEC.

Phishing (B)is a broader term but typically involvesmassfraudulent emails rather than targeted executive impersonation.

Brand impersonation (C)involves faking a company's identity (e.g., fake PayPal emails).

Pretexting (D)involves social engineering tactics but does not necessarily involve email compromise.

Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

NEW QUESTION: 111

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.

B. Data is being exfiltrated.

C. A logic bomb is deleting data.

D. Ransomware is encrypting files.

Answer: B (LEAVE A REPLY)

Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn't Real - This Time

NEW QUESTION: 112
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: 113
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 (D)is the most effective way to preventinjection attacks, such asSQL injection, XSS, etc. It ensures that only correctly formatted and expected inputs are processed by the application.
This is clearly identified underDomain 2.3: Application security techniques, whereinput validationis listed as aprimary defense against injection attacks.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Input validation: Prevents injection and malformed data attacks."

NEW QUESTION: 114
Which of the following security controls would best guard a payroll system against insider manipulation threats?
A. Compensating
B. Deterrent
C. Detective
D. Corrective
Answer: C (LEAVE A REPLY)
Detective controls (such as audit logs, monitoring, and alerts) are specifically designed to identify and reveal unauthorized or malicious activity, including insider manipulation, in systems like payroll. These controls help ensure that any attempts to manipulate data are discovered and investigated.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.3: "Detective controls monitor and identify violations or malicious activity after they have occurred." Exam Objectives 3.3: "Summarize various security control types and methods."

NEW QUESTION: 115

A security engineer needs to quickly identify a signature from a known malicious file. Which of the following analysis methods would the security engineer most likely use?

A. Static

B. Sandbox

C. Network traffic

D. Package monitoring

Answer: A (LEAVE A REPLY)

Static analysis is the process of examining a file without executing it to identify known malicious signatures, suspicious patterns, strings, embedded resources, or code fragments. When a security engineer needs to quickly extract a signature from a known malicious file, static analysis is the most efficient approach. This method allows analysts to inspect binary code, metadata, file headers, and hashes such as MD5/SHA-256.

According to Security+ SY0-701, static analysis is ideal for identifying:

* Malware signatures
* Embedded malicious payloads
* Hash values for detection
* Known indicators of compromise (IOCs)

Sandboxing (B) is used to observe behavior by executing the malware, which takes longer and is unnecessary when the malware is already known. Network traffic analysis (C) is used to observe communications, not generate file signatures. Package monitoring (D) refers to monitoring OS-level changes and system calls, which is a dynamic method.

Static analysis aligns with the requirement for quick identification, making option A the correct choice.

NEW QUESTION: 116

Which of the following risk management strategies is being used when a Chief Information Security Officer ignores known vulnerabilities identified during a risk assessment?

A. Transfer

B. Avoid

C. Mitigate

D. Accept

Answer: D (LEAVE A REPLY)

The correct answer is Accept because knowingly choosing not to address identified vulnerabilities is a formal example of risk acceptance. In the Security+ SY0-701 risk management framework, accepting risk means that leadership is aware of a vulnerability and its potential impact but decides to take no corrective action. This decision is typically based on factors such as cost, operational constraints, low likelihood of exploitation, or limited business impact.

Risk acceptance is a deliberate management decision, not an oversight. When a Chief Information Security Officer ignores known vulnerabilities identified during a risk assessment, the organization is implicitly acknowledging the risk and choosing to tolerate it. The SY0-701 study guide emphasizes that risk acceptance must be informed and approved by appropriate leadership, as accountability remains with the organization if the risk materializes.

Option A, Transfer, is incorrect because transferring risk involves shifting responsibility to a third party, such as purchasing cyber insurance or outsourcing services. Option B, Avoid, refers to eliminating risk entirely by discontinuing the risky activity, system, or process. Option C, Mitigate, involves implementing security controls to reduce the likelihood or impact of the risk, such as patching vulnerabilities or adding compensating controls.

Accepting risk does not mean the vulnerability is harmless; it means leadership has determined that addressing it is not justified at that time. The SY0-701 objectives highlight that accepted risks should be documented, reviewed periodically, and reassessed as conditions change, especially if threat likelihood or business impact increases.
In summary, ignoring known vulnerabilities after a risk assessment reflects a conscious decision to tolerate potential loss rather than reduce or eliminate it. This aligns directly with the risk acceptance strategy, making Option D the correct answer.

NEW QUESTION: 117
To which of the following security categories does an EDR solution belong?
A. Managerial
B. Technical
C. Physical
D. Operational
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following can automate vulnerability management?
A. CVE
B. SCAP
C. OSINT
D. CVSS
Answer: B (LEAVE A REPLY)
SCAP (Security Content Automation Protocol) is designed to automate vulnerability management, configuration assessment, and compliance checking. According to CompTIA Security+ SY0-701, SCAP standardizes how vulnerability information is expressed, measured, and shared, allowing security tools to automatically scan systems, identify weaknesses, and assess compliance against predefined baselines.
SCAP integrates multiple standards such as CVE, CVSS, CPE, and XCCDF, enabling automated vulnerability scanning, scoring, and reporting across large environments. This makes it a core technology for continuous vulnerability management and compliance automation.
CVE (A) is a catalog of known vulnerabilities, not an automation framework. OSINT (C) provides publicly available intelligence but does not automate remediation or assessment. CVSS (D) provides severity scoring but does not automate vulnerability management.
Because SCAP enables automated identification, assessment, and reporting of vulnerabilities, the correct answer is B: SCAP.

NEW QUESTION: 119
Which of the following receives logs from various devices and services, and then presents alerts?
A. SIEM
B. SCADA
C. SNMP
D. SCAP
Answer: (SHOW ANSWER)
A SIEM (Security Information and Event Management) system aggregates logs from diverse sources, analyzes them, and generates alerts on suspicious activities. It provides centralized monitoring and incident detection.
SCADA (B) is industrial control, SNMP (C) is a protocol for network management, and SCAP (D) is a standard for security content automation.
SIEMs are foundational in Security Operations monitoring#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 120
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. GRE
B. SD-WAN
C. EAP
D. IPSec
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Which of the following will harden access to a new database system? (Select two)
A. Jump server
B. NIDS
C. Monitoring
D. Proxy server
E. Host-based firewall
F. WAF
Answer: (SHOW ANSWER)
Hardening access to a new database system requires implementing controls that restrict and secure how administrators and applications connect to the database. A jump server (A) is a hardened intermediary system used to manage access to sensitive systems such as databases. By forcing administrators to authenticate through a controlled, monitored jump host instead of connecting directly, organizations reduce attack surfaces and prevent unauthorized lateral movement. Security+ SY0-701 identifies jump servers as critical in securing high-value systems.
A host-based firewall (E) provides system-level traffic filtering directly on the database server. It allows only trusted IPs, ports, and services to communicate with the database, significantly reducing exposure. This is an essential hardening measure because databases should only accept connections from specific application servers or administrative hosts.
NIDS (B) monitors traffic but does not harden access. Monitoring (C) provides visibility but does not restrict access. A proxy server (D) is not typically used for database access. A WAF (F) protects web applications, not internal database systems.
Thus, A (Jump server) and E (Host-based firewall) are the correct hardening controls.

NEW QUESTION: 122
A security manager is implementing MFA and patch management. Which of the following would best describe the control type and category? (Select two).
A. Physical

B. Managerial
C. Detective
D. Administrator
E. Preventative
F. Technical
Answer: E,F (LEAVE A REPLY)
Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.
References:
CompTIA Security+ SY0-701 Course Content: Domain 1: General Security Concepts, and Domain 4: Identity and Access Management, which cover the implementation of preventative and technical controls.

NEW QUESTION: 123
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: A (LEAVE A REPLY)

NEW QUESTION: 124
Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?
A. Configure all systems to log scheduled tasks.
B. Collect and monitor all traffic exiting the network.
C. Block traffic based on known malicious signatures.
D. Install endpoint management software on all systems.
Answer: (SHOW ANSWER)
Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 137 1

NEW QUESTION: 125
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: 126
Which of the following is the best reason to perform a tabletop exercise?
A. To address audit findings
B. To collect remediation response times
C. To update the IRP
D. To calculate the ROI
Answer: C (LEAVE A REPLY)
A tabletop exercise simulates incident scenarios to test and validate the effectiveness of an organization's Incident Response Plan (IRP), identifying gaps and areas needing updates. It promotes team readiness without disrupting operations.
Addressing audit findings (A), collecting remediation times (B), and calculating ROI (D) are separate activities and not the primary purpose of tabletop exercises.
This practice is an integral part of Security Operations and Incident Response training in SY0-701#6:Chapter
14 CompTIA Security+ Study Guide#.

NEW QUESTION: 127
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. Third-party attestation
B. Vulnerability scans
C. Penetration testing
D. Internal auditing
Answer: (SHOW ANSWER)

NEW QUESTION: 128
In which of the following scenarios is tokenization the best privacy technique 10 use?
A. Providing pseudo-anonymization tor social media user accounts
B. Serving as a second factor for authentication requests
C. Enabling established customers to safely store credit card Information
D. Masking personal information inside databases by segmenting data
Answer: C (LEAVE A REPLY)
Tokenization is a process that replaces sensitive data, such as credit card information, with a non-sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment information because the token can be safely stored and transmitted without exposing the original credit card number.
References =

* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Data Protection.

NEW QUESTION: 129
A Chief Information Security Officer (CISO) has developed information security policies that relate to the software development methodology.
Which of the following would the CISO most likely include in the organization's documentation?
A. Secrets management configurations
B. Branch protection tests
C. Peer review requirements
D. Multifactor authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?
A. Password spraying
B. Account forgery
C. Pass-t he-hash
D. Brute-force
Answer: (SHOW ANSWER)
Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords12.
The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3.
Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.
Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.
Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single

common password against multiple accounts5. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1: Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute ForceAttack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

NEW QUESTION: 131
An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?
A. DLP
B. SNMP traps
C. SCAP
D. IPS
Answer: A (LEAVE A REPLY)
The administrator is using a Data Loss Prevention (DLP) tool, which is designed to identify, monitor, and protect sensitive data. By fingerprinting specific files, DLP ensures that these files cannot be emailed or sent outside the organization without triggering an alert or blocking the action. This is a key feature of DLP systems, which prevent data exfiltration and ensure data security compliance.
* SNMP traps are used for network management and monitoring, not data protection.
* SCAP (Security Content Automation Protocol) is a set of standards for automating vulnerability management and policy compliance, unrelated to file monitoring.
* IPS (Intrusion Prevention System) blocks network-based attacks but does not handle file fingerprinting.

NEW QUESTION: 132
Which of the following is most likely to be used as a just-in-time reference document within a security operations center?
A. Change management policy
B. Risk profile
C. Playbook
D. SIEM profile
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A playbook is a step-by-step, just-in-time reference used by Security Operations Center (SOC) analysts when responding to security alerts, incidents, and suspicious activities. Playbooks provide documented procedures for common scenarios such as malware detection, phishing investigations, ransomware response, and account compromise.
According to the CompTIA Security+ SY0-701 exam framework, playbooks support incident response by reducing analyst guesswork and ensuring consistency. They include details such as triage steps, required tools, escalation paths, log sources, and containment actions. This makes playbooks the most suitable document for immediate reference during live investigations.
Change management policies (A) govern system or configuration changes, not SOC operations. Risk profiles (B) provide organizational risk overviews, not incident-response steps. SIEM profiles (D) define correlation rules or dashboards but are not procedural guides.
Therefore, the correct answer is playbooks, which enable efficient, standardized, and repeatable responses to operational security events.

NEW QUESTION: 133
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. Cold site
C. Recovery site
D. Warm site
Answer: (SHOW ANSWER)

NEW QUESTION: 134
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: C (LEAVE A REPLY)
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: 135
A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added. Which of the following would be the best solution to meet these objectives?
A. Load balancing
B. Fault tolerance
C. Proxy servers
D. Replication
Answer: (SHOW ANSWER)
Detailed Explanation:Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "High Availability Solutions".

NEW QUESTION: 136
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: 137
Which of the following describes the category of data that is most impacted when it is lost?
A. Public
B. Confidential
C. Private
D. Critical
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
The security team at a large global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?
A. Packet capture
B. Endpoint logs
C. OS security logs
D. Vulnerability scan
Answer: A (LEAVE A REPLY)
Packet capture data can be very large and may not need to be stored for extended periods compared to other logs essential for security audits.

NEW QUESTION: 139
The Chief Information Security Officer of an organization needs to ensure recovery from ransomware would likely occur within the organization's agreed-upon RPOs end RTOs. Which of the following backup scenarios would best ensure recovery?
A. Hourly differential backups stored on a local SAN array
B. Dally full backups stored on premises in magnetic offline media
C. Daly differential backups maintained by a third-party cloud provider
D. Weekly full backups with daily incremental stored on a NAS drive
Answer: D (LEAVE A REPLY)

A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Disaster Recovery and Backup Strategies.

NEW QUESTION: 140
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: 141
The security team notices that the Always On VPN solution sometimes fails to connect. This leaves remote users unprotected because they cannot connect to the on-premises web proxy. Which of the following changes will best provide web protection in this scenario?
A. Implement network access control.
B. Configure the local gateway to point to the VPN.
C. Create a public NAT to the on-premises proxy.
D. Install a host-based content filtering solution.
Answer: (SHOW ANSWER)
Installing a host-based content filtering solution on the endpoints ensures that web traffic is filtered locally even when the VPN connection to the on-premises proxy fails, maintaining protection for remote users.
Network access control (A) manages device network access, local gateway configuration (B) does not solve protection if VPN fails, and public NAT (C) exposes internal resources and increases risk.
Endpoint filtering complements VPN for resilient web security, covered in Security Architecture and Operations#6:Chapter 11 CompTIA Security + Study Guide#.

NEW QUESTION: 142
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: 143
A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?
A. Validate the code signature.
B. Execute the code in a sandbox.
C. Search the executable for ASCII strings.
D. Generate a hash of the files.
Answer: (SHOW ANSWER)
Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin.References:
CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 144
The number of tickets the help desk has been receiving has increased recently due to numerous false-positive phishing reports. Which of the following would be best to help to reduce the false positives?
A. Performing more phishing simulation campaigns
B. Improving security awareness training
C. Hiring more help desk staff
D. Implementing an incident reporting web page
Answer: B (LEAVE A REPLY)
Improving security awareness training directly addresses user behavior by teaching employees how to better recognize legitimate emails versus actual phishing attempts. Enhanced training can reduce the number of false positives by helping users more accurately identify true phishing attempts, lowering unnecessary reports and thus help desk workload.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.5: "Improved security awareness training helps reduce false positives in user reporting by teaching users to accurately identify phishing attempts." Exam Objectives 5.5: "Summarize security awareness and training techniques."

NEW QUESTION: 145

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: (SHOW ANSWER)

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: 146

A company wants to use new Wi-Fi-enabled environmental sensors in order to automatically collect metrics.

Which of the following will the security team most likely do?

A. Add the sensor software to the risk register.

B. Create a VLAN for the sensors.

C. Physically air gap the sensors.

D. Configure TLS 1.2 on all sensors.

Answer: (SHOW ANSWER)

Because these are Wi-Fi-enabled environmental sensors, they are effectively IoT/embedded devices that often have limited security controls, inconsistent patch support, and may expose management interfaces or services.

A common Security+ best practice is to reduce their attack surface and limit lateral movement by placing them in a separate, protected network segment and tightly controlling what they can talk to (for example, only to the metrics collector/broker). The Study Guide explicitly calls out VLAN-based segmentation for IoT as a hardening technique: "A common technique used in hardening networks is the use of VLANs... Placing IoT devices on a separate, protected VLAN with appropriate access controls... can help to ensure that frequently vulnerable devices are more protected." It also reinforces this in a practice question scenario: "What security control should she recommend...? ... Deploy the IoT devices to a protected VLAN." Why the other options are less likely:

* A (risk register) is governance documentation, not the most likely immediate technical control for deployment.
* C (air gap) is usually unrealistic for Wi-Fi sensors that must transmit metrics.
* D (TLS 1.2) may be beneficial, but many sensors can't support strong crypto consistently; segmentation is the most broadly applicable first move to contain risk.

References: CompTIA Security+ Study Guide (SY0-701) - Network Hardening/VLAN segmentation guidance ; related IoT hardening practice question recommending a protected VLAN .

NEW QUESTION: 147

An analyst identifies that multiple users have the same passwords, but the hashes appear to be completely different. Which of the following most likely explains this issue?

A. Data masking

B. Salting

C. Key escrow
D. Tokenization
Answer: (SHOW ANSWER)
Salting involves adding a unique value (salt) to each password before hashing it. This means that even if two users have the same password, the added salts ensure their hash values are different. This protects against attacks that exploit identical hash values, such as rainbow table attacks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Salting passwords ensures that identical passwords do not have identical hashes, even if the same hash algorithm is used." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 148
Which of the following is the best method to reduce the attack surface of an enterprise network?
A. Change default passwords for network printers.
B. Use port security for wired connections.
C. Create a guest wireless network for visitors.
D. Disable unused network services on servers.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following describes the procedures a penetration tester must follow while conducting a test?
A. Rules of engagement
B. Rules of acceptance
C. Rules of understanding
D. Rules of execution
Answer: A (LEAVE A REPLY)
Detailed Explanation:Rules of engagement specify the agreed-upon boundaries, scope, and procedures for a penetration test to ensure compliance and avoid disruption to the environment. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Penetration Testing Procedures".

NEW QUESTION: 150
A security analyst is prioritizing vulnerability scan results using a risk-based approach. Which of the following is the most efficient resource for the analyst to use?
A. Business impact analysis
B. Common Vulnerability Scoring System
C. Risk register
D. Exposure factor
Answer: (SHOW ANSWER)
TheCommon Vulnerability Scoring System (CVSS)is astandardized framework for assessing the severity of vulnerabilities. It provides a numerical score (0-10) based on factors such asexploitability, impact, and complexity, helping security analystsprioritize remediation efforts based on risk.
Business impact analysis (A)helps identifycritical business functionsbut does not specificallyprioritize vulnerabilities.

Risk register (C)tracks identified risks but does not classify vulnerabilities.
Exposure factor (D)is used inquantitative risk assessmentbut is not an industry standard for vulnerability prioritization.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Risk Management domain.

NEW QUESTION: 151
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: (SHOW ANSWER)
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.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, which includes secure communication protocols like SRTP for protecting data in transit.

NEW QUESTION: 152
Which of the following is the best safeguard to protect against an extended power failure?
A. Off-site backups
B. Batteries
C. Uninterruptible power supplies
D. Generators
Answer: D (LEAVE A REPLY)
For extended power failures, the best safeguard is a generator. CompTIA Security+ SY0-701 emphasizes that generators are designed to provide long-term, sustained power, unlike UPS systems, which only supply temporary emergency power.
Generators ensure that critical operations-including data centers, communication systems, and security infrastructure-stay online for hours or days, depending on fuel capacity. This matches the requirement for mitigating "extended" outages.
UPS units (C) protect against short-term outages and provide time for graceful shutdown or generator startup, but cannot support prolonged power consumption. Batteries (B) provide the least protection and run out quickly. Off-site backups (A) do not maintain operational continuity; they simply preserve data.

Disaster recovery and business continuity planning in SY0-701 highlights generators as essential components for maintaining availability, a core principle of the CIA triad. Generators prevent downtime, maintain productivity, and keep essential systems functioning throughout prolonged outages, making D the best answer.

NEW QUESTION: 153
Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?
A. Policies and procedures
B. Business impact analysts
C. Asset management
D. Vulnerability assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
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: 155
Which of the following methods to secure data is most often used to protect data in transit?
A. Encryption
B. Obfuscation
C. Permission restrictions
D. Hashing
Answer: A (LEAVE A REPLY)
Encryption is the standard method for protecting data in transit, ensuring that intercepted communications cannot be read without the appropriate decryption key.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3: "Encryption protects data confidentiality, especially for data in transit over networks." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 156
A security analyst investigates abnormal outbound traffic from a corporate endpoint. The traffic is encrypted and uses non-standard ports. Which of the following data sources should the analyst use first to confirm whether this traffic is malicious?
A. Application logs
B. Vulnerability scans
C. Endpoint logs
D. Packet captures
Answer: C (LEAVE A REPLY)
When investigating abnormal outbound traffic originating from a specific endpoint, endpoint logs are the most appropriate first data source to review. According to CompTIA Security+ SY0-701, endpoint logs provide detailed visibility into process execution, user actions, service creation, network connections initiated by applications, and security agent detections. This context is critical for determining which process initiated the encrypted traffic and why it is using non-standard ports.
Because the traffic is encrypted, packet captures (D) would reveal limited payload information and are more resource-intensive. Endpoint logs can quickly identify suspicious executables, command-line arguments, parent-child process relationships, and persistence mechanisms that indicate malware or command-and- control activity. Modern EDR tools rely heavily on endpoint telemetry for exactly this reason.
Application logs (A) may be useful later but are limited to specific applications. Vulnerability scans (B) identify weaknesses, not active malicious behavior.

Security+ SY0-701 emphasizes starting investigations as close to the suspected source as possible. Since the activity originates from a corporate endpoint, endpoint logs provide the fastest and most relevant confirmation of whether the traffic is malicious.

NEW QUESTION: 157
A financial institution would like to store its customer data m the cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution Is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would best meet the requirement?
A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral
Answer: C (LEAVE A REPLY)
Homomorphic encryption allows data to be encrypted and manipulated without needing to decrypt it first.
This cryptographic technique would allow the financial institution to store customer data securely in the cloud while still permitting operations like searching and calculations to be performed on the encrypted data. This ensures that the cloud service provider cannot decipher the sensitive data, meeting the institution's security requirements.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptographic Techniques.

NEW QUESTION: 158
A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?
A. Packet captures
B. Vulnerability scans
C. Metadata
D. Dashboard
Answer: D (LEAVE A REPLY)
A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12.
A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13.
A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards - SY0-601 CompTIA Security+ 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464:
CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

NEW QUESTION: 159
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: A (LEAVE A REPLY)
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: 160
A network security analyst monitors the network's IDS, which has flagged unusual activity. The IDS has detected multiple login attempts to a database server within a short period. These attempts come from various IP addresses that are not normally recognized by the network's usual traffic patterns. Each attempt uses the same username and password. Based on the following log output (corrected formatting for readability):
2025-04-10 14:22:01.4532 - Source IP: 192.168.15.101 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:02.1122 - Source IP: 192.168.15.102 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:02.7835 - Source IP: 192.168.15.103 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:03.5637 - Source IP: 192.168.15.104 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:04.9474 - Source IP: 192.168.15.105 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:05.5673 - Source IP: 192.168.15.106 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:06.1573 - Source IP: 192.168.15.107 - Status: Failed - User: JDoe - Action: Login Attempt
2025-04-10 14:22:07.7462 - Source IP: 192.168.15.108 - Status: Failed - User: JDoe - Action: Login Attempt Which of the following types of network attacks is most likely occurring?
A. Cross-site scripting
B. Credential replay
C. Distributed denial of service
D. SQL injection
Answer: B (LEAVE A REPLY)
The pattern shows rapid, repeated authentication attempts against a database server using the same username (JDoe) and the same password, originating from multiple different IP addresses in a short window. Among the choices, this most closely aligns with a credential replay style attack (often discussed as replaying captured authentication material or repeatedly reusing stolen credentials) rather than an application-layer injection (SQLi/XSS) or a volumetric availability attack (DDoS). The Study Guide describes credential replay as follows: "Credential replay

attacks are a form of network attack that requires the attacker to be able to capture valid network data and to re-send it or delay it so that the attacker's own use of the data is successful." In practice, defenders may see replay-like behavior when an attacker (or botnet) repeatedly tries the same captured credential pair (or captured authentication artifact) from different sources. The multiple IPs can indicate automation or distributed infrastructure used to evade rate limits and lockout controls. The other options don't fit the evidence: XSS requires script injection into web content; SQL injection would show suspicious SQL payloads, not repeated logins; DDoS focuses on overwhelming availability and typically shows traffic floods rather than repeated authentication attempts using a single account credential set.
Therefore, the best answer is credential replay.
References: Credential replay definition and explanation .

NEW QUESTION: 161
A new employee can select a particular make and model of an employee workstation from a preapproved list.
Which of the following is this an example of?
A. MDM
B. CYOD
C. PED
D. COPE
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
The described scenario is CYOD (Choose Your Own Device). In a CYOD model, employees may choose from a list of company-approved devices. These devices are vetted for compatibility, security, and organizational standards while still providing some flexibility to employees.
The SY0-701 exam differentiates CYOD from other mobile deployment models:
COPE (D) - Company-Owned, Personally Enabled: devices are company-owned and fully managed, but employees can use them personally.
MDM (A) - Mobile Device Management: a tool, not a deployment model, used for managing configurations and security on devices.
PED (C) - Portable Electronic Device: a generic category, not a deployment strategy.
CYOD strikes a balance between employee preference and maintaining a secure, standardized environment. It reduces risk associated with BYOD while avoiding the rigidity of COPE. CYOD also supports consistent patching, support, and security enforcement because all devices meet the organization's baseline criteria.
This aligns with the Security Architecture section of SY0-701, where the exam stresses secure device deployment strategies and maintaining uniform controls over endpoint assets.

NEW QUESTION: 162
Which of the following should a systems administrator use to decrease the company's hardware attack surface?
A. Replication
B. Isolation
C. Centralization
D. Virtualization
Answer: (SHOW ANSWER)
Virtualization (D)allows multiple systems and services to be hosted onfewer physical machines, therebyreducing the total number of physical devicesand consequently thehardware attack surface. This also allows for better patching, monitoring, and control.
The fewer devices you manage physically, the fewer entry points there are for attackers to exploit hardware- level vulnerabilities.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Reducing attack surface: Use of virtualization to consolidate systems."

NEW QUESTION: 163
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. Reviewing email policies
B. Recognizing phishing
C. Using password management
D. Providing situational awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which of the following are the most important considerations when encrypting data? (Select two).
A. Obfuscation
B. Algorithms
C. Data masking
D. Key length
E. Tokenization
F. Salting
Answer: B,D (LEAVE A REPLY)
When encrypting data, two fundamental drivers of cryptographic strength are the algorithm you choose and the key length you use (which affects brute-force feasibility and overall security margin). The Study Guide emphasizes algorithm selection as a best practice: "First, choose your encryption system wisely... Choose an encryption system with an algorithm in the public domain that has been thoroughly vetted by industry experts." It then highlights key selection/size as another central decision: "You must also select your keys in an appropriate manner. Use a key length that balances your security requirements with performance considerations." These two choices directly affect whether encryption meaningfully protects confidentiality. By contrast, obfuscation, masking, and tokenization are different data-protection techniques (often used to reduce exposure or de-identify data) rather than core encryption-strength parameters. Salting is primarily associated with strengthening password hashing (defending against rainbow table attacks), not selecting encryption primitives /strength for general data encryption. Therefore, the best two considerations in the context of encryption itself are Algorithms and Key length.
References: Encryption best practices-select vetted algorithms and appropriate key length .

NEW QUESTION: 165
An organization is looking to optimize its environment and reduce the number of patches necessary for operating systems. Which of the following will best help to achieve this objective?
A. Containers
B. Microservices
C. Virtualization
D. Real-time operating system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166

The Chief Information Security Officer gives the security community the opportunity to report vulnerabilities on the organization's public-facing assets. Which of the following does this scenario best describe?

A. Bug bounty

B. Red teaming

C. Open-source intelligence

D. Third-party information sharing

Answer: (SHOW ANSWER)

This scenario describes a bug bounty program, which invites external security researchers to responsibly identify and report vulnerabilities in an organization's systems. CompTIA Security+ SY0-701 defines bug bounty programs as structured initiatives that reward researchers for discovering and disclosing security flaws before they can be exploited by malicious actors.

Bug bounty programs extend security testing beyond internal teams and provide continuous, real-world testing of public-facing assets. They are particularly effective for identifying zero-day vulnerabilities, logic flaws, and edge-case issues that automated tools may miss.

Red teaming (B) is a controlled, internal or contracted adversarial exercise, not an open invitation. Open- source intelligence (C) involves gathering publicly available information, not vulnerability reporting. Third- party information sharing (D) refers to sharing threat intelligence, not soliciting vulnerability reports.

Because the CISO is inviting the broader security community to report vulnerabilities, the correct answer is A: Bug bounty.

NEW QUESTION: 167

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: 168

Which of the following is a benefit of vendor diversity?

A. Zero-day resiliency
B. Load balancing
C. Secure configuration guide applicability
D. Patch availability
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Which of the following provides resilience by hosting critical VMs within different IaaS providers while being maintained by internal application owners?
A. Multicloud architectures
B. SaaS provider diversity
C. On-premises server load balancing
D. Corporate-owned, off-site locations
Answer: A (LEAVE A REPLY)
Multicloud architectures use two or more IaaS providers (e.g., AWS + Azure + GCP) to distribute workloads, increase redundancy, and reduce single points of failure. Security+ SY0-701 emphasizes multicloud strategies for enhancing:
Resilience
Availability
Fault tolerance
Geographic redundancy
Vendor independence
The question specifies:
Critical VMs
Hosted across different IaaS providers
Still maintained by internal application owners
This perfectly matches a multicloud deployment, where organizations maintain control over VM configuration while leveraging multiple cloud vendors for resilience.
SaaS provider diversity (B) applies to application services, not internally managed VMs.
On-prem load balancing (C) does not involve cloud providers.
Corporate-owned off-site locations (D) refer to DR sites, not multi-vendor cloud hosting.
Thus, A: Multicloud architectures is the correct answer.

NEW QUESTION: 170
A malicious insider from the marketing team alters records and transfers company funds to a personal account. Which of the following methods would be the best way to secure company records in the future?
A. Hashing
B. Permission restrictions
C. Input validation
D. Access control list
Answer: D (LEAVE A REPLY)

NEW QUESTION: 171
A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?
A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions
Answer: A (LEAVE A REPLY)
Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed. References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 17-18, 372-373

NEW QUESTION: 172
Which of the following security controls is a company implementing by deploying HIPS? (Select two)
A. Directive
B. Preventive
C. Physical
D. Corrective
E. Compensating
F. Detective
Answer: B,F (LEAVE A REPLY)
A Host-based Intrusion Prevention System (HIPS) provides both preventive and detective security controls.
Security+ SY0-701 describes HIPS as a host-level security solution that monitors system behavior, blocks malicious activity, and logs suspicious events.
It functions as a preventive control (B) because it can:
* Stop malware execution
* Block unauthorized changes
* Prevent exploit attempts
* Enforce endpoint protection policies
It is also a detective control (F) because it can:
* Record attempted attacks
* Identify suspicious activities
* Generate alerts for security teams
Directive controls (A) refer to policies; physical controls (C) refer to locks and barriers; corrective controls (D) restore systems after an incident; compensating controls (E) substitute for missing primary controls.

Therefore, the two correct answers are B (Preventive) and F (Detective).

NEW QUESTION: 173
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. Refect
C. Accept
D. Transfer
Answer: (SHOW ANSWER)

NEW QUESTION: 174
The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?
A. Fines
B. Reputational damage
C. Sanctions
D. Contractual implications
Answer: (SHOW ANSWER)
The most direct and immediate consequence of non-compliance with local data privacy regulations is fines.
CompTIA Security+ SY0-701 emphasizes that privacy and data protection laws (such as GDPR, HIPAA, or regional privacy statutes) include explicit financial penalties for organizations that fail to meet compliance requirements. These fines are measurable, enforceable, and frequently cited by regulators as primary enforcement mechanisms.
While reputational damage (B) and contractual implications (D) are serious secondary effects, they are indirect and harder to quantify. Sanctions (C) typically apply in geopolitical or trade contexts rather than routine privacy enforcement. Boards of directors are often most responsive to clearly defined financial exposure; fines provide a concrete, defensible rationale for allocating additional budget to compliance, tooling, staffing, and process improvements.
Security+ SY0-701 highlights risk communication to executives using quantifiable impacts. Presenting the likelihood and magnitude of regulatory fines directly supports a cost-benefit analysis and demonstrates fiduciary responsibility. Therefore, A: Fines is the most appropriate consequence to present.

NEW QUESTION: 175
An administrator has configured a quarantine subnet for all guest devices that connect to the network. Which of the following would be best for the security team to configure on the MDM before allowing access to corporate resources?
A. Device fingerprinting
B. Compliance attestation
C. NAC
D. 802.1X
Answer: (SHOW ANSWER)

Compliance attestation (B)ensures that devices meetpredefined security policies(e.g., encryption enabled, updated antivirus, latest OS patches) before being allowed access to corporate resources. This is commonly enforced usingMobile Device Management (MDM)systems.
By using compliance checks via MDM, only secure,policy-compliantdevices are promoted from quarantine to trusted network segments.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.2 - "MDM, NAC, and compliance enforcement: Compliance attestation before access."

NEW QUESTION: 176
Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?
A. Non-repudiation
B. Integrity
C. Confidentiality
D. Availability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 177
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: C (LEAVE A REPLY)
Full Disk Encryption (FDE) ensures that all data on the drive is encrypted, preventing unauthorized access even if the device is lost.

NEW QUESTION: 178
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: 179

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies

B. Version control

C. Input validation

D. Code signing

Answer: (SHOW ANSWER)

Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users.

Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

NEW QUESTION: 180

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile.

Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation

B. Identity proofing

C. Password complexity

D. Default password changes

E. Password manager

F. Open authentication

Answer: (SHOW ANSWER)

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them.

Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

NEW QUESTION: 181

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories

B. Dark web

C. Threat feeds
D. State actors
E. Vulnerability databases
Answer: A (LEAVE A REPLY)
Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is critical for protecting against this type of leakage.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

NEW QUESTION: 182
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. Time-based access control
B. Role-based access control
C. Digital rights management
D. Network access control
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following is the best way to prevent an unauthorized user from plugging a laptop into an employee's phone network port and then using tools to scan for database servers?
A. MAC filtering
B. Segmentation
C. Certification
D. Isolation
Answer: A (LEAVE A REPLY)
Detailed Explanation:MAC filtering allows network administrators to control device access by specifying allowed MAC addresses. This prevents unauthorized devices, such as a laptop plugged into a network port, from gaining access. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats and Vulnerabilities, Section: "Network Access Control Methods".

NEW QUESTION: 184

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: D (LEAVE A REPLY)
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: 185
The analyst wants to move data from production to the UAT server for testing the latest release. Which of the following strategies to protect data should the analyst use?
A. Data masking
B. Data tokenization
C. Data obfuscation
D. Data encryption
Answer: A (LEAVE A REPLY)
Data masking replaces sensitive data with realistic but fictional data, preserving format and usability while protecting confidential information during testing in environments like UAT (User Acceptance Testing).
Tokenization (B) replaces data with tokens but is more common for payment data in production. Obfuscation (C) scrambles data but is less structured than masking. Encryption (D) protects data confidentiality but may not be practical for testing.
Data masking is a best practice for protecting sensitive data in non-production environments covered in the General Security Concepts domain#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 186
A database administrator is updating the company's SQL database, which stores credit card information for pending purchases. Which of the following is the best method to secure the data against a potential breach?
A. Masking
B. Tokenization
C. Hashing
D. Obfuscation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
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. Pivoting

C. Port scanning
D. Exploit validation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
A security analyst wants to better understand the behavior of users and devices in order to gain visibility into potential malicious activities. The analyst needs a control to detect when actions deviate from a common baseline Which of the following should the analyst use?
A. Antivirus
B. Endpoint detection and response
C. Sandbox
D. Intrusion prevention system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 189
A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team. Which of the following should the company implement to meet this requirement?
A. VDI
B. MDM
C. VPN
D. VPC
Answer: A (LEAVE A REPLY)
Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server.
Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company's infrastructure without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company's secure servers.
References =
* CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

NEW QUESTION: 190
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?
A. SPF
B. GPO
C. NAC
D. FIM
Answer: D (LEAVE A REPLY)
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

Some of the benefits of FIM are:
It can prevent data tampering and corruption by verifying the checksums or hashes of the files.
It can identify the source and time of the changes by logging the user and system actions.
It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.
It can support forensic analysis and incident response by providing evidence and audit trails of the changes.
References:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3:
Security Tools, p. 209-210
CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective
2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

NEW QUESTION: 191
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: 192

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: C,D (LEAVE A REPLY)

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: 193

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: 194

A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

A. Logging all NetFlow traffic into a SIEM

B. Deploying network traffic sensors on the same subnet as the servers

C. Logging endpoint and OS-specific security logs

D. Enabling full packet capture for traffic entering and exiting the servers

Answer: D (LEAVE A REPLY)

Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

NEW QUESTION: 195
A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).
A. Key escrow
B. TPM presence
C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking
Answer: A,B (LEAVE A REPLY)
Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.
TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

NEW QUESTION: 196
Attackers created a new domain name that looks similar to a popular file-sharing website. Which of the following threat vectors is being used?
A. Watering-hole attack
B. Brand impersonation
C. Phishing
D. Typosquatting
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
The scenario describes attackers registering a similar-looking domain to trick users into visiting a malicious site. This matches the definition of typosquatting, also known as URL hijacking or domain spoofing.
Typosquatting relies on users mistyping legitimate URLs or failing to notice slight visual differences (e.g., "dropbx.com" instead of "dropbox.com"). Attackers use these domains to distribute malware, steal credentials, or redirect users to phishing pages.
Watering-hole attacks (A) infect legitimate websites frequented by a specific target group, which does not match this scenario. Brand impersonation (B) involves mimicking a company's identity-often combined with email phishing-but the question specifically mentions creating a similar-looking domain, which is characteristic of typosquatting. Phishing (C) may use these malicious domains, but phishing is a broader social-engineering attack, whereas typosquatting precisely describes the domain manipulation technique.
Security+ SY0-701 emphasizes typosquatting under Social Engineering & Web-based Threats, highlighting how attackers exploit user errors to redirect traffic to malicious destinations. Reducing this risk involves user training, DNS filtering, domain monitoring, and certificate validation.

NEW QUESTION: 197
Which of the following should a security analyst consider when prioritizing remediation efforts against known vulnerabilities?
A. The impact of reporting to executive management
B. The overall organizational risk tolerance
C. Information gathered from open sources
D. The source of the reported risk
Answer: B (LEAVE A REPLY)
Organizational risk tolerance is the primary factor determining how quickly and aggressively vulnerabilities should be remediated. Security+ SY0-701 explains that organizations have different appetites for risk depending on business needs, regulatory expectations, operational constraints, and financial impact.
A company with low risk tolerance may prioritize almost every vulnerability and remediate quickly.
A company with high risk tolerance may delay or accept some lower-impact risks.
This consideration directly influences patch prioritization, resource allocation, and mitigation timelines.
Option A-executive reporting-does not influence technical prioritization.
Option C-open-source intelligence-helps identify vulnerabilities but does not determine urgency.
Option D-the source of the reported risk-is irrelevant; what matters is severity and business impact.
Thus, B: The overall organizational risk tolerance is the key factor for prioritizing remediation.

NEW QUESTION: 198
An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?
A. Vishing
B. Smishing
C. Pretexting
D. Phishing
Answer: B (LEAVE A REPLY)
Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences2

NEW QUESTION: 199

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: (SHOW ANSWER)
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: 200
Which of the following security measures is required when using a cloud-based platform for IoT management?
A. Encrypted connection
B. Single sign-on
C. Federated identity
D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 201
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: 202
Which of the following best describes a common use of OSINT?
A. Monitoring internal systems and network traffic to detect abnormal behavior
B. Installing and configuring security patches to fix known vulnerabilities
C. Collecting information from public platforms to find possible security exposures
D. Encrypting sensitive company data and storing it securely in the cloud
Answer: C (LEAVE A REPLY)
OSINT stands for open source intelligence and is commonly used to gather information from publicly available sources to support security activities such as reconnaissance, threat intelligence, and identifying exposures (for example, leaked credentials, exposed infrastructure details, or public references to vulnerabilities). The Practice Tests book defines OSINT directly: "OSINT, or open source intelligence, is intelligence information obtained from public sources like search engines, websites, domain name registrars, and a host of other locations." That definition aligns precisely with option C's "collecting information from public platforms." The Study Guide similarly explains OSINT in the threat intelligence context: "Open source threat intelligence is threat intelligence that is acquired from publicly available sources." This supports the idea that OSINT is used to discover relevant information that may affect security posture-such as indicators, exposed assets, or details useful for defensive planning. The other options describe different operational activities: A is internal monitoring (SIEM/IDS/EDR style), B is patch management, and D is encryption/storage strategy-none are
"open source intelligence."
References: OSINT definition as intelligence obtained from public sources ; OSINT as threat intelligence acquired from publicly available sources .

NEW QUESTION: 203
During a routine audit, an analyst discovers that a department uses software that was not vetted. Which threat is this?
A. Espionage
B. Data exfiltration
C. Shadow IT
D. Zero-day
Answer: C (LEAVE A REPLY)
Shadow IT refers to software, hardware, cloud services, or applications deployed without approval from the IT or security department. In this scenario, a high school department is using an unvetted simulation program-classic Shadow IT behavior.
Security+ SY0-701 explains that Shadow IT:
* Introduces unknown vulnerabilities
* Bypasses security controls

* Creates compliance risks
* Leads to data exposure
* Interferes with standard configuration management

Espionage (A) involves intelligence gathering, not unauthorized software use. Data exfiltration (B) involves data theft, not unauthorized software deployment. Zero-day (D) refers to unknown vulnerabilities, not unapproved systems.

Thus, Shadow IT is the correct answer.

NEW QUESTION: 204

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. Time of day

D. Discretionary

Answer: A (LEAVE A REPLY)

NEW QUESTION: 205

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: 206

A security manager wants to reduce the number of steps required to identify and contain basic threats. Which of the following will help achieve this goal?

A. SOAR

B. SIEM

C. DMARC

D. NIDS

Answer: A (LEAVE A REPLY)

SOAR (Security Orchestration, Automation, and Response) is designed to automate repetitive security tasks, orchestrate workflows, and reduce manual effort in identifying and containing threats. CompTIA Security+ SY0-701 describes SOAR as an advanced tool that integrates with SIEM, EDR, firewalls, and ticketing systems to automate detection, enrichment, and response actions.

By using SOAR playbooks, security teams can automate:

Initial threat triage

Log correlation

Host isolation

Indicator lookups

Ticket creation and escalation
This significantly reduces the number of manual steps an analyst must perform, achieving the manager's goal of streamlining threat-handling procedures.
A SIEM (B) centralizes logs and alerts but still requires manual investigation unless paired with SOAR.
DMARC (C) protects email domains from spoofing but does not automate threat response. NIDS (D) detects threats on the network but does not automate containment.
SOAR's ability to automate identification and response makes A the correct answer.

NEW QUESTION: 207
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: 208
Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?
A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition
Answer: (SHOW ANSWER)
A buffer overflow is a 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. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-
701 - 2.3 2

NEW QUESTION: 209
A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?
A. Host-based firewall
B. Web application firewall
C. Access control list
D. Application allow list
Answer: A (LEAVE A REPLY)
A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

NEW QUESTION: 210
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach that would affect offshore offices. Which of the following is this an example of?
A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response
Answer: A (LEAVE A REPLY)
A tabletop exercise is a discussion-based simulation in which stakeholders review and talk through their roles, responsibilities, and actions in response to a hypothetical incident. This allows participants to evaluate and improve response plans without actual disruption.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.6: "Tabletop exercises involve key stakeholders discussing roles, responsibilities, and actions in response to simulated incidents." Exam Objectives 5.6: "Given a scenario, implement security incident management processes."

NEW QUESTION: 211
An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions over the phone to use a new account. Which of the following would most likely prevent this activity in the future?
A. Standardizing security incident reporting
B. Executing regular phishing campaigns
C. Implementing insider threat detection measures
D. Updating processes for sending wire transfers
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:

Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) canprevent fraudulenttransactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.
Standardizing security incident reportingis useful for tracking security events but does not prevent fraud in real time.
Executing regular phishing campaignsimproves awareness but does not enforce a verification process for financial transactions.
Implementing insider threat detectionfocuses on internal risks but does not specifically prevent external fraud.
Amore secure wire transfer processwith additional verification steps is the most effective measure against fraudulent transactions.

NEW QUESTION: 212
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: (SHOW ANSWER)
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: 213
A company asks a vendor to help its internal red team with a penetration test without providing too much detail about the infrastructure. Which of the following penetration testing methods does this scenario describe?
A. Passive reconnaissance
B. Partially-known environment
C. Integrated testing
D. Defensive testing
Answer: B (LEAVE A REPLY)

This scenario describes a partially-known environment penetration test. In CompTIA Security+ SY0-701, penetration testing approaches are commonly categorized as black box (unknown), white box (fully known), and gray box (partially known). A partially-known environment means the tester is given limited information-enough to be realistic and efficient, but not complete details about the infrastructure.
Here, the vendor is assisting an internal red team and is intentionally not provided with extensive infrastructure details, which mirrors a gray-box testing approach. This method balances realism and efficiency by simulating an attacker who has some knowledge (such as credentials, architecture diagrams, or application details) but not full access or documentation.
Passive reconnaissance (A) is an activity within testing, not a testing methodology. Integrated testing (C) refers to coordinated testing involving multiple teams (e.g., red and blue teams) with full cooperation.
Defensive testing (D) focuses on validating defensive controls rather than simulating an attacker's perspective.
Therefore, the correct answer is B: Partially-known environment.

NEW QUESTION: 214
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

NEW QUESTION: 215
Which of the following should be used to ensure a device is inaccessible to a network-connected resource?
A. Disablement of unused services
B. Web application firewall
C. Host isolation
D. Network-based IDS
Answer: (SHOW ANSWER)
Detailed Explanation:Host isolation ensures that a device is separated from the network, preventing it from accessing or being accessed by other network resources. This is typically achieved by quarantining the device.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Isolation and Containment".

NEW QUESTION: 216
A company discovered its data was advertised for sale on the dark web. During the initial investigation, the company determined the data was proprietary data. Which of the following is the next step the company should take?
A. Notify the applicable parties of the breach.
B. Implement vulnerability scanning of the company's systems.

C. Report the breach to the local authorities.
D. Identity the attacker sentry methods.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?
A. Zero-day attacks
B. Insider threats
C. End-of-life support
D. Known exploits
Answer: (SHOW ANSWER)
Applying the latest OS updates, patches, and endpoint definitions is the most effective way to prevent known exploits, which are attacks leveraging previously discovered vulnerabilities for which fixes are available.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Applying patches and updates prevents exploitation of known vulnerabilities."
Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

NEW QUESTION: 218
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 thesecurity 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: 219
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: (SHOW ANSWER)
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: 220
Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A. Destruction
B. Certification
C. Retention
D. Sanitization
Answer: (SHOW ANSWER)
Detailed Explanation:
Retention policies dictate how long data must be stored to comply with local and international regulations.
Non-compliance can result in legal and financial penalties. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Retention and Legal Requirements".

NEW QUESTION: 221
Which of the following activities are associated with vulnerability management? (Select two).

A. Reporting
B. Correlation
C. Containment
D. Tabletop exercise
E. Prioritization
F. Exploiting
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 222
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: B (LEAVE A REPLY)
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: 223
Which of the following is a directive managerial control?
A. Acceptable use policy
B. Login warning banner
C. Master service agreement
D. No trespassing sign
Answer: A (LEAVE A REPLY)

A directive managerial control provides guidance and expectations for behavior through policy and governance. An Acceptable Use Policy (AUP) is a classic example, as it defines how users may and may not use organizational systems and data. Security+ SY0-701 categorizes policies as managerial (administrative) controls that direct user behavior and establish accountability.
A login warning banner (B) is typically a deterrent/administrative control but is not managerial in nature. A master service agreement (C) is a contractual/legal document, not a managerial directive for internal users. A
"No trespassing" sign (D) is a physical deterrent control.
Because an AUP formally directs behavior and is enforced through management processes, A: Acceptable use policy is correct.

NEW QUESTION: 224
A group of developers has a shared backup account to access the source code repository. Which of the following is the best way to secure the backup account if there is an SSO failure?
A. RAS
B. EAP
C. SAML
D. PAM
Answer: D (LEAVE A REPLY)
Detailed Explanation:Privileged Access Management (PAM) solutions enhance security by enforcing strong authentication, rotation of credentials, and access control for shared accounts. This is especially critical in scenarios like SSO failures. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Privileged Access and Identity Management".

NEW QUESTION: 225
A company is experiencing issues with employees leaving the company for a competitor and taking customer contact information with them. Which of the following tools will help prevent this from reoccurring?
A. FIM
B. NAC
C. IDS
D. UBA
Answer: D (LEAVE A REPLY)
User Behavior Analytics (UBA) monitors user activities and detects anomalous behavior such as unauthorized data access or exfiltration, including when employees attempt to copy sensitive customer contact information before leaving. UBA can alert security teams to insider threats proactively.
File Integrity Monitoring (FIM) (A) detects unauthorized changes to files but is less effective against data exfiltration by insiders. Network Access Control (NAC) (B) controls device access to the network, and Intrusion Detection Systems (IDS) (C) detect suspicious network activity but do not specifically analyze user behaviors.
UBA is a critical tool for insider threat detection covered in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 226
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: 227
Which of the following phases of the incident response process attempts to minimize disruption?
A. Recovery
B. Containment
C. Preparation
D. Analysis
Answer: B (LEAVE A REPLY)
Containmentis the phase wherean organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.
Recovery (A)focuses on restoring normal operations after an incident.
Preparation (C)involves planning and readiness before an incident occurs.
Analysis (D)involvesinvestigating the root causeand assessing the damage.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

NEW QUESTION: 228
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. IPS
B. SIEM
C. SASE
D. CASB
Answer: C (LEAVE A REPLY)

The requirements point to a cloud-delivered, remote-user-first architecture that provides secure connectivity and security controls as an integrated service. Secure Access Service Edge (SASE) matches this because it combines remote connectivity capabilities (often replacing or modernizing traditional VPN approaches) with cloud-based security services, including firewalling, in a way that supports distributed users and resilient global access. The Study Guide explicitly states: "Secure Access Service Edge (SASE...) combines virtual private networks, SD-WAN, and cloud-based security tools like firewalls, cloud access security brokers (CASBs), and zero-trust networks to provide secure access for devices regardless of their location." This directly aligns with a fully remote workforce ("regardless of their location"), VPN capability, and an integrated firewall ("cloud-based security tools like firewalls").
Why the other options don't fit as well: IPS is a specific protective control, not an end-to-end remote access architecture; SIEM is for log aggregation/correlation and monitoring, not VPN + firewall delivery; and CASB is a component used to enforce cloud policy, but the guide distinguishes it as a policy enforcement point rather than a full connectivity + firewall architecture: "A CASB is a policy enforcement point..." .
Therefore, SASE is the best match.
References: Sybex CompTIA Security+ Study Guide (SY0-701) - SASE definition and included capabilities (also duplicated in).

NEW QUESTION: 229
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: D (LEAVE A REPLY)
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: 230
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: 231
An administrator is installing an SSL certificate on a new system. During testing, errors indicate that the certificate is not trusted. The administrator has verified with the issuing CA and has validated the private key.
Which of the following should the administrator check for next?
A. If the root certificate is installed
B. If the certificate signing request is valid
C. If the wildcard certificate is configured
D. If the public key is configured
Answer: A (LEAVE A REPLY)

NEW QUESTION: 232
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. User provisioning
B. Federation
C. Security groups
D. Vertical scaling
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
Which of the following can be used to compromise a system that is running an RTOS?
A. Replay attack
B. Memory injection
C. Ransomware
D. Cross-site scripting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 234
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: D (LEAVE A REPLY)
The correct answer is Maintenance window because firmware upgrades on critical infrastructure devices, such as routers, must be performed during a predefined and approved time period to minimize operational impact.
Within the Security+ SY0-701 objectives, maintenance windows are a key component of change management and operational security, ensuring that potentially disruptive changes occur when business risk is lowest.
Upgrading router firmware often requires rebooting the device, which can temporarily interrupt network connectivity. A maintenance window defines when this downtime is acceptable, ensures stakeholders are notified in advance, and allows rollback plans to be executed if the upgrade

fails. The SY0-701 study guide stresses that scheduled maintenance windows reduce the risk of unplanned outages, service-level agreement violations, and user disruption while supporting system stability and availability.
Option A, Software development life cycle, applies to the design, development, testing, and deployment of software applications, not routine infrastructure maintenance tasks like firmware updates. Option B, Risk tolerance, refers to an organization's willingness to accept risk and guides decision-making at a strategic level, but it does not dictate the procedural steps of performing an upgrade. Option C, Certificate signing request, is used when requesting digital certificates from a certificate authority and is unrelated to firmware updates.
Following a maintenance window aligns with best practices emphasized in SY0-701 for managing operational risk, preserving availability, and enforcing structured change control. It ensures proper approvals, testing, monitoring, and backout plans are in place before changes are introduced into production environments.
In summary, firmware upgrades are operational changes that can affect availability. Performing them during an approved maintenance window is essential to maintaining reliable network operations and reflects Security+ SY0-701 best practices for secure and controlled system management.

NEW QUESTION: 235
A security team receives reports about high latency and complete network unavailability throughout most of the office building. Flow logs from the campus switches show high traffic on TCP 445. Which of the following is most likely the root cause of this incident?
A. Buffer overflow
B. NTP amplification attack
C. Worm
D. Kerberoasting attack
Answer: C (LEAVE A REPLY)
Port 445 is used by the SMB protocol on Windows systems. Large volumes of unexpected traffic on TCP 445 are commonly associated with worms that exploit SMB vulnerabilities (such as WannaCry or NotPetya).
Worms are self-replicating malware that spread rapidly across a network, consuming bandwidth, causing high latency, and often resulting in network outages. This matches the scenario given, where network unavailability and abnormal port 445 traffic are observed.
References:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1, "Malware Types: Worms" CompTIA Security+ Exam Objectives: 2.1 CompTIA Glossary: "Worm-A self-replicating malware that spreads across networks, often exploiting vulnerabilities such as those in SMB (TCP 445)."

NEW QUESTION: 236
After completing an annual external penetration test, a company receives the following guidance:
* Decommission two unused web servers currently exposed to the internet.
* Close 18 open and unused ports found on their existing production web servers.
* Remove company email addresses and contact info from public domain registration records.
Which of the following does this represent?
A. Attack surface reduction
B. Vulnerability assessment
C. Tabletop exercise
D. Business impact analysis
Answer: A (LEAVE A REPLY)

The guidance focuses on attack surface reduction by eliminating unnecessary services, closing unused ports, and limiting publicly available information that attackers could leverage. Reducing the attack surface lowers the organization's exposure to threats and potential entry points.
Vulnerability assessments (B) identify weaknesses but do not necessarily involve active reduction measures.
Tabletop exercises (C) simulate incidents, and business impact analysis (D) assesses the effects of disruptions, neither of which match the described activities.
Attack surface reduction is a core principle in Security Operations and penetration testing remediation strategies in SY0-701#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 237
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4:
Architecture and Design, pages 164-1652.

NEW QUESTION: 238
Which of the following is a vulnerability concern for end-of-life hardware?
A. Failure to follow hardware disposal procedures could result in unintended data release.
B. The supply chain may not have replacement hardware.
C. Newly released software may require computing resources not available on legacy hardware.
D. The vendor may stop providing patches and updates.
Answer: (SHOW ANSWER)

The most significant vulnerability concern for end-of-life (EOL) hardware is that vendors stop providing patches and updates. CompTIA Security+ SY0-701 highlights that unsupported hardware and software no longer receive security fixes, leaving known vulnerabilities permanently unpatched. This creates an expanding attack surface that adversaries can easily exploit.
Once hardware reaches EOL status, newly discovered vulnerabilities will remain unaddressed, increasing the likelihood of compromise. This is especially dangerous for systems exposed to networks or handling sensitive data, where exploitation can lead to data breaches, lateral movement, or service disruption.
Option A relates to disposal risks, not active vulnerabilities. Option B is a logistical issue, not a security vulnerability. Option C is a compatibility concern, not a direct vulnerability.
Because unpatched systems are inherently vulnerable and cannot be secured through updates, the correct answer is D: The vendor may stop providing patches and updates.

NEW QUESTION: 239
Which of the following is used to quantitatively measure the criticality of a vulnerability?
A. CVE
B. CVSS
C. CIA
D. CERT
Answer: (SHOW ANSWER)
CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality.
CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors. The other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39

NEW QUESTION: 240
A security analyst identifies an incident in the network. Which of the following incident response activities would the security analyst perform next?
A. Containment
B. Detection
C. Eradication
D. Recovery
Answer: (SHOW ANSWER)
Once an incident is detected, the next step is containment, which involves limiting the scope and impact of the incident to prevent further damage. Containment can be temporary or long-term, isolating affected systems or networks.
Detection (B) is the initial identification phase before containment. Eradication (C) follows containment and involves removing the root cause. Recovery (D) is the final step to restore normal operations.
This workflow is fundamental in the Incident Response lifecycle detailed in Security Operations in SY0-701
#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 241

Which of the following exercises should an organization use to improve its incident response process?
A. Tabletop
B. Replication
C. Failover
D. Recovery
Answer: A (LEAVE A REPLY)
A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures.
It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

NEW QUESTION: 242
Which of the following data recovery strategies will result in a quick recovery at low cost?
A. Hot
B. Cold
C. Manual
D. Warm
Answer: D (LEAVE A REPLY)
A warm site offers a compromise between cost and recovery speed. It includes hardware and network infrastructure partially configured, allowing quicker recovery than a cold site but at lower cost than a hot site.
Hot sites (A) enable rapid recovery but at high cost. Cold sites (B) are low cost but slow to recover. Manual (C) refers to manual processes, typically slower.
Warm sites balance recovery time and cost in disaster recovery planning#6:Chapter 9 CompTIA Security+ Study Guide#.

NEW QUESTION: 243
Which of the following methods will 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 effective method for identifying legacy systems within an environment.

Vulnerability scanners assess hosts for outdated operating systems, unsupported software versions, missing patches, deprecated services, and known Common Vulnerabilities and Exposures (CVEs). CompTIA Security+ SY0-701 highlights vulnerability scanning as a foundational security operation used to gain visibility into system age, patch status, and configuration weaknesses.
Legacy systems often stand out in scan results because they run end-of-life operating systems, use deprecated protocols, or lack current security updates. These indicators allow security teams to quickly flag systems that require isolation, compensating controls, or replacement.
Bug bounty programs (A) rely on external researchers and are not designed to inventory internal assets.
Package monitoring (C) tracks software behavior and changes but does not identify system age or support status. Dynamic analysis (D) evaluates running applications for vulnerabilities, not infrastructure lifecycle status.
Because vulnerability scans provide broad visibility into system versions and supportability, the correct answer is B: Vulnerability scan.

NEW QUESTION: 244
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?
A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the 'deny any* policy prior to enabling the new policy
D. Including an 'allow any1 policy above the 'deny any* policy
Answer: (SHOW ANSWER)
A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the 'deny any' policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network.
Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it.
Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic.
Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers.
Including an 'allow any' policy above the 'deny any' policy would not prevent the issue, and it would render the 'deny any' policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An 'allow any' policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the 'deny any' policy, which is to block any traffic that does not match any of the previous rules. Moreover, an 'allow any' policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network. References = CompTIA Security+ SY0-701 Certification Study Guide, page 204-205; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

NEW QUESTION: 245
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: 246
After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?
A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling
Answer: C (LEAVE A REPLY)
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

NEW QUESTION: 247
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 that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
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 the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 248
A security analyst created a fake account and saved the password in a non-readily accessible directory in a spreadsheet. An alert was also configured to notify the security team if the spreadsheet is opened. Which of the following best describes the deception method being deployed?
A. Honeypot
B. Honey account
C. Honeytoken

D. Honeynet

Answer: C (LEAVE A REPLY)

A honeytoken is a form of deception technology in which a fake asset (such as credentials, files, or database records) is planted in a system or network to detect unauthorized access or malicious activity. The fake password stored in a hidden spreadsheet, with monitoring for access, is a classic example of a honeytoken. It is not an interactive system (like a honeypot or honeynet) but rather a marker or tripwire intended to alert the security team to suspicious behavior. This method helps identify attackers and their methods early in the intrusion process.

References:

CompTIA Security+ SY0-701 Official Study Guide, Domain 1.1, "Deception and Disruption Technologies" CompTIA Security+ Exam Objectives: 1.1 CompTIA Glossary: "Honeytoken-A fictitious record or file intended to attract or identify unauthorized access."

NEW QUESTION: 249

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

A. To gather loCs for the investigation

B. To discover which systems have been affected

C. To eradicate any trace of malware on the network

D. To prevent future incidents of the same nature

Answer: D (LEAVE A REPLY)

Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization.

Root cause analysis is not meant to gather loCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security + Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

NEW QUESTION: 250

Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?

A. IDS

B. Honeypot

C. Layer 3 switch

D. Firewall

Answer: B (LEAVE A REPLY)

NEW QUESTION: 251

A service provider wants a cost-effective way to rapidly expand from providing internet links to managing them. Which of the following methods will allow the service provider to best scale its services while maintaining performance consistency?

A. Escalation support

B. Increased workforce

C. Baseline enforcement
D. Technical debt
Answer: (SHOW ANSWER)
Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost- effective expansion.
Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.
Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 252
During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?
A. Whaling
B. Credential harvesting
C. Prepending
D. Dumpster diving
Answer: D (LEAVE A REPLY)
Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security measures in cyber hygiene practices.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

NEW QUESTION: 253
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: (SHOW ANSWER)
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: 254
A systems administrator needs to provide traveling employees with a tool that will protect company devices regardless of where they are working. Which of the following should the administrator implement?
A. Isolation
B. Segmentation
C. ACL
D. HIPS
Answer: D (LEAVE A REPLY)
A Host-based Intrusion Prevention System (HIPS) protects individual devices by monitoring and preventing malicious activity directly on the host. It is ideal for protecting traveling employees' devices outside the corporate network.
Isolation (A) and segmentation (B) apply to networks, and ACL (Access Control List) (C) restricts network traffic but does not provide host-level protection.
HIPS is emphasized in Security Operations for endpoint protection#6:Chapter 11 CompTIA Security+ Study Guide#.

NEW QUESTION: 255
Which of the following would best prepare a security team for a specific incident response scenario?
A. Situational awareness
B. Risk assessment
C. Root cause analysis
D. Tabletop exercise
Answer: (SHOW ANSWER)
ATabletop exercise (D)is adiscussion-based simulationof an incident scenario. It allows security teams towalk through procedures, responsibilities, and communicationsin alow-pressure environment, improving readiness without impacting operations.
It is specifically designed toprepare teams for real-world incident handling.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response plans and exercises: Tabletop exercises."

NEW QUESTION: 256
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 followingmostlikely 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: (SHOW ANSWER)

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+ StudyGuide 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: 257
A security administrator observed the following in a web server log while investigating an incident:

```
"GET ../../../../etc/passwd"
```

Which of the following attacks did the security administrator most likely see?
A. Brute force
B. Directory traversal
C. Credential replay
D. Privilege escalation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 258
An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned. one of the batch jobs talked and caused a major disruption. Which of the following would work best to prevent this type of incident from reoccurring?
A. Job rotation
B. Retention
C. Outsourcing
D. Separation of duties
Answer: (SHOW ANSWER)
Job rotation is a security control that involves regularly moving employees to different roles within an organization. This practice helps prevent incidents where a single employee has too much control or knowledge about a specific job function, reducing the risk of disruption when an employee leaves. It also helps in identifying any hidden issues or undocumented processes that could cause problems after an employee's departure.
References:

* CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which includes job rotation as a method to ensure business continuity and reduce risks.

NEW QUESTION: 259
Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?
A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit
Answer: B (LEAVE A REPLY)
Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market.
Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data. References = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

NEW QUESTION: 260
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. Threshold
B. Appetite
C. Avoidance
D. Register
Answer: (SHOW ANSWER)
Risk appetiterefers to thelevel of risk an organization is willing to acceptbefore implementing security measures. When expanding access controls, the company must assess how much risk is acceptable in terms ofdata exposure, unauthorized access, and compliance obligations.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Risk Management domain.

NEW QUESTION: 261
Which of the following phases of an incident response involves generating reports?
A. Recovery
B. Preparation
C. Lessons learned
D. Containment
Answer: C (LEAVE A REPLY)
The lessons learned phase of an incident response process involves reviewing the incident and generating reports. This phase helps identify what went well, what needs improvement, and what changes should be made to prevent future incidents. Documentation and reporting are essential parts of this phase to ensure that the findings are recorded and used for future planning.

* Recovery focuses on restoring services and normal operations.
* Preparation involves creating plans and policies for potential incidents, not reporting.
* Containment deals with isolating and mitigating the effects of the incident, not generating reports.

NEW QUESTION: 262
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: (SHOW ANSWER)
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 HardwareSecurity?
Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, :
Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION: 263
The private key for a website was stolen, and a new certificate has been issued. Which of the following needs to be updated next?
A. CRL
B. CSR
C. OCSP
D. SCEP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 264
Following a security review, an organization must ensure users verify their identities against the company's identity services with individual credentials leveraging WPA2-Enterprise for wireless access. Which of the following configuration steps correctly applies RADIUS in this environment?
A. Enabling 802.1X authentication and integrating it with the corporate directory
B. Installing self-signed certificates on all user devices
C. Enabling MAC filters for all wireless clients

D. Configuring the wireless controller to require multifactor authentication

Answer: A (LEAVE A REPLY)

WPA2-Enterprise is designed for environments where users authenticate with unique, individual credentials backed by an enterprise identity store, rather than a shared preshared key. The Study Guide explicitly states:

"WPA2-Enterprise relies on a RADIUS authentication server as part of an 802.1X implementation for authentication. Users can thus have unique credentials and be individually identified." That maps directly to the requirement that users verify identity against the company's identity services using individual credentials.

It further explains how this is implemented operationally: "802.1X is an IEEE standard for access control...

In wireless networks, 802.1X is used to integrate with RADIUS servers, allowing enterprise users to authenticate and gain access to the network." Therefore, the correct configuration step is enabling 802.1X and tying authentication into the organization's identity source (commonly a corporate directory). The other choices don't correctly "apply RADIUS" for WPA2-Enterprise: self-signed certs are not universally required for all EAP types and can introduce trust issues; MAC filters are weak and spoofable; and MFA might be beneficial but is not the fundamental step that enables RADIUS-backed WPA2-Enterprise authentication.

References: WPA2-Enterprise uses RADIUS + 802.1X and supports unique user credentials ; 802.1X integrates wireless authentication with RADIUS .

NEW QUESTION: 265

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: (SHOW ANSWER)

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: 266

A few weeks after deploying additional email servers, employees complain that messages are being marked as spam. Which needs to be updated?

A. CNAME

B. SMTP

C. DLP

D. SPF

Answer: D (LEAVE A REPLY)

SPF (Sender Policy Framework) DNS records specify which mail servers are authorized to send email on behalf of a domain. When new email servers are added but SPF records are not updated, recipient mail systems cannot verify the legitimacy of the new servers. As a result, those messages are flagged as spam or rejected altogether.

CompTIA Security+ SY0-701 highlights SPF as an essential email authentication mechanism used to reduce spoofing, phishing, and spam classification errors. Updating the SPF record to include the new servers ensures email reputation is maintained and messages are delivered properly.
CNAME (A) maps hostnames but does not affect outbound email legitimacy. SMTP (B) is the mail protocol, not the authentication method. DLP (C) governs sensitive data handling, not spam classification.
Thus, SPF is the correct answer.

NEW QUESTION: 267
Which of the following is a preventive physical security control?
A. Alarm system
B. Motion sensors
C. Video surveillance system
D. Bollards
Answer: (SHOW ANSWER)

NEW QUESTION: 268
A security team wants to work with the development team to ensure WAF policies are automatically created when applications are deployed.
Which concept describes this capability?
A. IaC
B. IoT
C. IoC
D. IaaS
Answer: A (LEAVE A REPLY)
The ability to automatically generate WAF (Web Application Firewall) policies during application deployment is a characteristic of Infrastructure as Code (IaC). IaC allows infrastructure components-such as firewalls, WAF policies, load balancers, and security groups-to be defined, version-controlled, and deployed programmatically.
According to Security+ SY0-701, IaC enhances DevSecOps workflows by embedding security controls directly into deployment pipelines, ensuring consistent, repeatable, and automated application protection. This reduces human error, eliminates configuration drift, and ensures that every new application instance is deployed with the correct WAF rules already in place.
IoT (B) involves connected devices.
IoC (C) refers to Indicators of Compromise.
IaaS (D) provides cloud infrastructure but does not itself automate security policy generation.
Thus, A: IaC is the correct concept enabling automated WAF policy creation.

NEW QUESTION: 269
Which of the following is the main consideration when a legacy system that is a critical part of a company's infrastructure cannot be replaced?
A. Complexity
B. Cost
C. Resource provisioning
D. Single point of failure
Answer: D (LEAVE A REPLY)

NEW QUESTION: 270
A company's web filter is configured to scan the URL for strings and deny access when matches are found.
Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?
A. encryption=off\
B. http://
C. www.*.com
D. :443
Answer: B (LEAVE A REPLY)
A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling",
"porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port
/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or
?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.
To
prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.
The other options are not correct because they do not match the protocol of non-encrypted web traffic.
Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page
69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION: 271
Which of the following threat actors is themostlikely 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: 272

Which of the following should an internal auditor check for first when conducting an audit of the organization' s risk management program?

A. Policies and procedures

B. Asset management

C. Vulnerability assessment

D. Business impact analysis

Answer: (SHOW ANSWER)

An internal audit of a risk management program typically starts by verifying the organization has the governance foundation that defines how risk is managed, documented, approved, and monitored. That foundation is established in policies and procedures, which set expectations, roles, and the required workflow for consistent risk practices (for example: how risks are identified, who owns them, how they are tracked, and how exceptions are handled). The Study Guide emphasizes that policy is central to governance: "Policy serves as one of the primary governance tools for any cybersecurity program, setting out the principles and rules that guide the execution of security efforts throughout the enterprise." Without policies/procedures, the auditor cannot reliably assess whether asset management, vulnerability assessments, or BIAs are being performed according to an established, repeatable process-or whether results are being used appropriately in risk decisions. Asset management and vulnerability assessments provide critical inputs to risk identification and assessment, and the BIA supports impact determination and recovery planning, but an auditor usually first confirms that the organization's documented governance structure exists and is being followed so the rest of the program can be evaluated against those requirements.

References: Governance and policy as the primary tool guiding cybersecurity program execution .

NEW QUESTION: 273

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: (SHOW ANSWER)
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

NEW QUESTION: 274
The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the best option?
A. Warm site
B. Cold site
C. Hot site
D. Failover site
Answer: B (LEAVE A REPLY)

NEW QUESTION: 275
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: (SHOW ANSWER)
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: 276
Which of the following is prevented by proper data sanitization?
A. Hackers' ability to obtain data from used hard drives
B. Devices reaching end-of-life and losing support
C. Disclosure of sensitive data through incorrect classification
D. Incorrect inventory data leading to a laptop shortage
Answer: A (LEAVE A REPLY)
Detailed Explanation:Proper data sanitization ensures that sensitive data is securely erased from storage devices, preventing unauthorized access or recovery when the devices are disposed of or reused. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Sanitization and Disposal Methods".

NEW QUESTION: 277
Which of the following threat actors would most likely target an organization by using a logic bomb within an internally-developed application?
A. Nation-state
B. Trusted insider
C. Organized crime group
D. Hacktivist
Answer: B (LEAVE A REPLY)
A logic bomb is a malicious code segment hidden inside legitimate software that triggers under specific conditions (dates, system states, user actions). Because logic bombs require direct access to source code or the development environment, the most likely attacker is a trusted insider-especially a disgruntled developer or administrator with the ability to modify internal applications.
Security+ SY0-701 emphasizes that insider threats have:
Elevated access
Knowledge of internal systems
Ability to manipulate production code
Motivation driven by revenge, termination, or personal grievances
These factors make insiders uniquely capable of embedding logic bombs into internally-developed applications.
Nation-state actors (A) typically target critical infrastructure or advanced espionage, not internal business apps. Organized crime groups (C) seek financial gain and generally do not have internal code access.
Hacktivists (D) focus on ideological disruption, typically through external attacks, not internal code manipulation.
Thus, the threat actor most likely to plant a logic bomb in internal software is B: Trusted insider.

NEW QUESTION: 278

A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

A. Internal audit

B. Attestation

C. Due diligence

D. Penetration testing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 279

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: 280

A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

A. Hashes

B. Certificates

C. Algorithms

D. Salting

Answer: A (LEAVE A REPLY)

Posting hashes allows users to verify the integrity of downloaded files. As outlined in Security+ SY0-701, a cryptographic hash (e.g., SHA-256) produces a fixed-length digest unique to the file's contents. Users can compute the hash of the downloaded file and compare it to the published value; a match confirms the file has not been altered.

Certificates (B) establish identity and trust but do not directly verify file integrity post-download unless combined with signing workflows.

Algorithms (C) are general methods, not verification artifacts. Salting (D) is used with password hashing and is irrelevant here.

Therefore, A: Hashes is the correct choice.

NEW QUESTION: 281

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: 282
A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured. Which of the followingbestdescribes what the security analyst should do to identify this behavior?

A. [Digital forensics

B. E-discovery

C. Incident response

D. Threat hunting

Answer: D (LEAVE A REPLY)

Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements. References = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701), Chapter 4: Threat Detection and Response, page 153. Threat Hunting - SY0-701 CompTIA Security + : 4.1, Video 3:18. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

NEW QUESTION: 283

Which of the following outlines the configuration, maintenance, and security roles between a cloud service provider and the customer?

A. Service-level agreement

B. Responsibility matrix

C. Memorandum of understanding

D. Non-disclosure agreement

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

A responsibility matrix, often referred to in cloud computing as the Shared Responsibility Model, defines the exact roles, duties, and expectations between a cloud service provider (CSP) and the customer. This includes who is responsible for configuration, maintenance, patching, logging, updates, identity management, network security, and data protection.

According to the SY0-701 exam objectives, cloud models such as SaaS, PaaS, and IaaS all divide responsibilities differently. The responsibility matrix clarifies these boundaries so that neither party assumes the other is handling a critical security task. Misunderstandings in these areas can create dangerous security gaps, such as unpatched virtual machines, misconfigured storage buckets, or weak access controls.

A Service-Level Agreement (A) focuses on uptime, performance, and service expectations-not shared security roles. A Memorandum of Understanding (C) describes high-level cooperation between organizations, while an NDA (D) protects confidential information.

The responsibility matrix is emphasized under Security Program Management, specifically in managing third- party relationships and cloud provider governance, ensuring both parties understand their obligations and reducing the risk of misconfigurations or operational vulnerabilities.

NEW QUESTION: 284

During a SQL update of a database, a temporary field used as part of the update sequence was modified by an attacker before the update completed in order to allow access to the system. Which of the following best describes this type of vulnerability?

A. Race condition

B. Memory injection

C. Malicious update

D. Side loading

Answer: A (LEAVE A REPLY)
Arace conditionoccurs whentwo or more processes attempt to access and modify a shared resource simultaneously, leading to unintended behavior. In this scenario, the attacker was able to modify a temporary fieldbefore the SQL update completed, indicating atime-of-check to time-of-use (TOCTOU) vulnerability, which is a type of race condition.
Memory injection (B)refers to inserting malicious code into a running process's memory, but that isnotwhat is happening here.
Malicious update (C)is too broad and does not specifically describe this scenario.
Side loading (D)is a technique where malicious software is loaded via a trusted application, unrelated to this case.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

NEW QUESTION: 285
A vendor needs to remotely and securely transfer files from one server to another using the command line.
Which of the following protocols should be Implemented to allow for this type of access? (Select two).
A. SSH
B. SNMP
C. RDP
D. S/MIME
E. SMTP
F. SFTP
Answer: A,F (LEAVE A REPLY)
Secure Shell (SSH) is a protocol used for secure command-line access to remote systems, while Secure File Transfer Protocol (SFTP) is an extension of SSH used specifically for securely transferring files. Both SSH and SFTP ensure that data is encrypted during transmission, protecting it from interception or tampering.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

NEW QUESTION: 286
A company receives an alert that a network device vendor, which is widely used in the enterprise, has been banned by the government.
Which of the following will the company's general counsel most likely be concerned with during a hardware refresh of these devices?
A. Sanctions
B. Data sovereignty
C. Cost of replacement
D. Loss of license
Answer: A (LEAVE A REPLY)
When the government bans a vendor, the primary concern for the company's general counsel is sanctions, which are legal restrictions that prohibit the purchase, use, import, or continued operation of products associated with restricted entities. Security+ SY0-701 stresses that compliance with government regulations and legal mandates is a critical oversight responsibility. Failure to comply may result in severe penalties, including fines, loss of contracting eligibility, and reputational damage.
During a hardware refresh, general counsel will ensure the organization is not violating federal trade sanctions, procurement laws, or export/import restrictions. Even if devices are already purchased, continued use may still violate the sanctions, creating legal liability.

Data sovereignty (B) relates to storage location requirements, not vendor bans. Cost of replacement (C) is an operational and financial concern, not a legal one. Loss of license (D) typically applies to software but is not the primary legal concern tied to a government-issued vendor ban. Therefore, sanctions are the general counsel's primary focus.

NEW QUESTION: 287
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)
Theprimary goal of corrective controls in financial systems is to ensure that errors do not propagate across interconnected systems. Financial transactions are ofteninterdependent, meaning one incorrect or unauthorized change can affect multiple systems. Regulations often mandate these controls tomaintain accuracy and prevent cascading failures.
A (insider threats altering banking details)is a concern, but thisscenario focuses on corrective controls, not insider threats specifically.
C (business insurance)is unrelated to why corrective controls are implemented.
D (preventing unauthorized changes)falls underpreventive, notcorrectivecontrols.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 288
Which of the following would be the greatest concern for a company that is aware of the consequences of non- compliance with government regulations?
A. Right to be forgotten
B. Sanctions
C. External compliance reporting
D. Attestation
Answer: B (LEAVE A REPLY)
Detailed Explanation:
Sanctions imposed for non-compliance can include fines, legal actions, and loss of business licenses. These pose a significant financial and reputational risk to organizations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Regulatory Compliance Risks".

NEW QUESTION: 289

Which solution is most likely used in the financial industry to mask sensitive data?
A. Tokenization
B. Hashing
C. Salting
D. Steganography
Answer: (SHOW ANSWER)
Tokenization replaces sensitive financial data-such as credit card numbers, account numbers, or customer identifiers-with harmless tokens that retain usability but reveal nothing if leaked. This is widely used in the financial industry, particularly in PCI-DSS-regulated systems.
Hashing (B) is one-way and not reversible, making it unsuitable for financial transactions that need original data retrieved. Salting (C) is used to protect hashed passwords, not to mask financial data. Steganography (D) hides data inside media files but is not used for payment processing.
Security+ SY0-701 identifies tokenization as the preferred method for protecting structured sensitive data while maintaining operational functionality.
Thus, the correct answer is A: Tokenization.

NEW QUESTION: 290
A Chief Information Officer wants to ensure that network devices cannot connect to the public internet and the local network to directly perform firmware updates. The IT team must manually perform the update process by using a portable device. Which of the following architecture types best fits this description?
A. Microservices
B. Air-gapped
C. Software-defined networking
D. Serverless
Answer: B (LEAVE A REPLY)
The correct answer is Air-gapped because this architecture deliberately isolates systems from external and internal networks to prevent any direct electronic communication. In the Security+ SY0-701 domain of Security Architecture, air-gapped environments are used to achieve the highest level of protection against network-based threats by physically or logically separating critical systems from untrusted networks such as the internet or even the organization's internal network.
In this scenario, the CIO requires that network devices cannot connect to the public internet or the local network for firmware updates, and that updates must be performed manually using a portable device. This is a defining characteristic of an air-gapped architecture. Air-gapped systems rely on controlled, manual transfer methods-such as USB drives or other removable media-to introduce updates, ensuring that malware, remote exploits, and supply-chain-based network attacks cannot reach the isolated systems through traditional network paths.
Option A, Microservices, refers to an application design model where software is built as loosely coupled services and does not address physical or logical network isolation. Option C, Software-defined networking, focuses on centralized and programmable network control, not network disconnection. Option D, Serverless, is a cloud computing model where infrastructure management is abstracted away from developers and is incompatible with isolated, offline environments.
The SY0-701 study guide highlights air-gapped architectures as common in high-security environments such as industrial control systems, military systems, financial infrastructure, and environments requiring maximum protection against zero-day exploits and remote compromise. While air-gapping introduces operational overhead and update delays, it significantly reduces attack surface and exposure to external threats.
In summary, an architecture that requires manual updates via portable media and prevents any direct network connectivity is best described as air-gapped, making option B the correct answer.

NEW QUESTION: 291
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 systemsisone of the most effective ways to reduce the attack surface.
Unsupported OS versionsno longer receive security patches, making them prime targets for attackers.
Removing outdated softwareensures 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 butdoes not address outdated vulnerabilities.
C (High availability)focuses on uptime, not security risk reduction.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

NEW QUESTION: 292
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. Patch installation
B. Full disk encryption
C. Telnet connection
D. SSH tunneling
Answer: (SHOW ANSWER)

NEW QUESTION: 293
A customer reports that software the customer downloaded from a public website has malware in it. However, the company that created the software denies any malware in its software at delivery time. Which of the following techniques will address this concern?
A. Secure storage
B. Static code analysis
C. Input validation
D. Code signing
Answer: D (LEAVE A REPLY)
Code signing uses digital signatures to verify software authenticity and integrity, ensuring the code has not been tampered with since it was signed by the developer. It helps detect if malware was introduced after delivery.
Static code analysis (B) inspects code for vulnerabilities during development but does not verify delivered binaries. Input validation (C) protects applications at runtime. Secure storage (A) protects stored data, unrelated to software delivery.
Code signing is an essential security control in Software Development Life Cycle and Supply Chain Security
#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 294

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

A. Target of evaluation

B. Resource reuse

C. SQL injection

D. Side loading

Answer: C (LEAVE A REPLY)

NEW QUESTION: 295

An employee decides to collect PII data from the company's system for personal use. The employee compresses the data into a single encrypted file before sending the file to their personal email. The security department becomes aware of the attempted misuse and blocks the attachment from leaving the corporate environment. Which of the following types of employee training would most likely reduce the occurrence of this type of issue?

(Select two).

A. Privacy legislation

B. Social engineering

C. Risk management

D. Company compliance

E. Phishing

F. Remote work

Answer: A,D (LEAVE A REPLY)

The misuse of personally identifiable information (PII) is often mitigated through employee training on privacy legislation and company compliance. Training on privacy legislation educates employees about legal requirements and consequences related to handling PII, such as GDPR or HIPAA. Company compliance training reinforces internal policies and procedures regarding data handling, acceptable use, and the repercussions of violations.

While social engineering and phishing training are important for security awareness, they address external threats rather than insider misuse of data. Risk management is a broader discipline focused on assessing and mitigating organizational risks but does not directly prevent employee misuse through training. Remote work training focuses on secure practices for working outside corporate environments, which is not the core issue here.

This approach aligns with Security Program Management and Oversight principles emphasizing compliance and privacy training to reduce insider threats#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 296

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat

B. Hacktivist

C. Nation-state

D. Organized crime

Answer: D (LEAVE A REPLY)

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17
1

NEW QUESTION: 297
A manufacturing organization receives the results from a penetration test. According to the results, legacy devices that are critical to continued business function display vulnerabilities. The devices have minimal vendor support and should be segmented and monitored closely. Which of the following devices were most likely identified?
A. Workstations
B. Embedded systems
C. Core router
D. DNS server
Answer: B (LEAVE A REPLY)
The scenario describes legacy, business-critical devices with minimal vendor support that must be segmented and closely monitored. This strongly matches embedded systems commonly found in manufacturing environments (e.g., industrial machinery controllers, sensors, ICS/SCADA components). The Study Guide defines embedded systems as: "Embedded systems are computer systems that are built into other devices.
Industrial machinery, appliances, and cars are all places where you may have encountered embedded systems." Manufacturing organizations often can't easily replace or patch these systems because they have long lifecycles and may depend on specialized firmware/RTOS and proprietary integrations. The same guide warns that legacy/unsupported platforms create risk due to lack of vendor security patches and recommends compensating controls: "Lack of support implies that no new security patches... will be released... In cases where the organization simply must continue using an unsupported operating system, best practice dictates isolating the system as much as possible... and applying as many compensating security controls as possible, such as increased monitoring and implementing strict network firewall rules." That guidance directly supports the question's "segmented and monitored closely" language. Workstations typically have stronger patch/support options; core routers and DNS servers are important, but they are not usually described as embedded legacy devices with minimal vendor support in a manufacturing context.
References: Embedded systems definition and manufacturing examples ; legacy/unsupported systems require isolation/monitoring compensating controls .

NEW QUESTION: 298
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.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

NEW QUESTION: 299
An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?
A. Content categorization
B. URL scanning
C. Centralized proxy
D. Agent-based
Answer: D (LEAVE A REPLY)

NEW QUESTION: 300
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: (SHOW ANSWER)

NEW QUESTION: 301
Which of the following most securely protects data at rest?
A. TLS 1.2
B. AES-256
C. Masking
D. Salting
Answer: (SHOW ANSWER)
AES-256 is a symmetric encryption algorithm widely used to protect data at rest by converting plaintext into ciphertext that is unreadable without the proper key. It provides strong confidentiality and is a standard for encrypting stored data.
TLS 1.2 (A) secures data in transit, not at rest. Masking (C) obscures data but typically for display or limited use and is reversible. Salting (D) is used alongside hashing to protect passwords and data integrity but does not encrypt data.
Encryption with AES-256 is recognized as a best practice for securing stored data in the Security+ Cryptography and General Security Concepts domains#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 302
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: 303
While a user reviews their email, a host gets infected by malware from an external hard drive plugged into the host. The malware steals all the user's credentials stored in the browser. Which of the following training topics should the user review to prevent this situation from reoccurring?
A. Operational security
B. Removable media and cables
C. Password management
D. Social engineering
Answer: B (LEAVE A REPLY)
Detailed Explanation:This scenario highlights the need for training on the secure use of removable media.
Users should learn to avoid using untrusted external storage devices to prevent malware infections. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Removable Media Controls and User Awareness Training".

NEW QUESTION: 304
An administrator investigating an incident is concerned about the downtime of a critical server due to a failed drive. Which of the following would the administrator use to estimate the time needed to fix the issue?
A. MTTR
B. MTBF
C. RTO
D. RPO
Answer: (SHOW ANSWER)
Mean Time To Repair (MTTR) is a key metric used to estimate the average time required to repair a failed component or system and restore it to operational status. In this case, the administrator would rely on MTTR to estimate how long it will take to fix the critical server's failed drive and get it back online.
Mean Time Between Failures (MTBF) measures the expected operational lifespan between failures, so it does not provide an estimate of repair time.
Recovery Time Objective (RTO) refers to the maximum allowable downtime for a system or service before unacceptable impact occurs, which is a planning metric rather than an actual repair time measure.

Recovery Point Objective (RPO) defines the maximum acceptable data loss measured in time and relates to backup frequency rather than repair duration.
Therefore, MTTR is the appropriate metric to estimate the time to fix a failed drive. This concept is detailed in the Resilience and Physical Security chapter within the Security Operations domain of the SY0-701 exam
#6:Chapter 9 CompTIA Security+ Study Guide#

NEW QUESTION: 305
Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?
A. Client
B. Third-party vendor
C. Cloud provider
D. DBA
Answer: (SHOW ANSWER)
According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on the cloud infrastructure. Therefore, the client is responsible for securing the company's database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security. References = CompTIA Security+ SY0-701 Certification Study Guide, page 263-264; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

NEW QUESTION: 306
A company evaluates several options that would allow employees to have remote access to the network. The security team wants to ensure the solution includes AAA to comply with internal security policies. Which of the following should the security team recommend?
A. Jump server with 802.1X
B. RDP connection with LDAPS
C. Web proxy for all remote traffic
D. IPSec with RADIUS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 307
A store is setting up wireless access for their employees. Management wants to limit the number of access points while ensuring all areas of the store are covered. Which of the following tools will help management determine the number of access points needed?
A. Signal locator
B. WPA3
C. Heat map
D. Site survey
Answer: D (LEAVE A REPLY)

A site survey is the formal assessment used to determine the optimal number and placement of wireless access points (APs). According to Security+ SY0-701, wireless site surveys evaluate factors such as building layout, RF interference, wall material density, antenna propagation, and signal overlap. The goal is to ensure full wireless coverage while minimizing the number of APs needed, maximizing performance, and reducing dead zones.
During a site survey, technicians analyze:
Signal strength patterns
Interference sources (microwaves, metal shelving, wiring, etc.)
Required coverage zones
Capacity needs (number of users, devices)
Although heat maps (C) visually represent wireless signal distribution, they are a result of a site survey, not the process itself. WPA3 (B) is a security protocol unrelated to determining coverage. A signal locator (A) is not an enterprise-grade planning tool.
Therefore, the correct answer is D: Site survey.

NEW QUESTION: 308
A security analyst is reviewing the following logs about a suspicious activity alert for a user's VPN log-ins.
Which of the following malicious activity indicators triggered the alert?
#Log Summary:
User logs in fromChicago, ILmultiple times, then suddenly a successful login appears fromRome, Italy, followed again by Chicago logins - all within ashort time span.
A. Impossible travel
B. Account lockout
C. Blocked content
D. Concurrent session usage
Answer: (SHOW ANSWER)
Impossible travel (A)refers to logins fromgeographically distant locations within a time period that makes travel between them physically impossible. In this case, a user logging in fromChicago and Rome within a short timeframetriggers this anomaly.
This is a strong indicator of acompromised accountorstolen credentialsbeing used elsewhere.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity:
Impossible travel (geolocation anomalies)."

NEW QUESTION: 309
Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?
A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation
Answer: C (LEAVE A REPLY)
Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure.
The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to

only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data.
Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare.
Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

NEW QUESTION: 310
A company wants to use new Wi-Fi-enabled environmental sensors to automatically collect metrics. Which of the following will the security team most likely do?
A. Add the sensor software to the risk register.
B. Create a VLAN for the sensors.
C. Physically air gap the sensors.
D. Configure TLS 1.2 on all sensors.
Answer: (SHOW ANSWER)
Creating a VLAN for Wi-Fi-enabled environmental sensors is the most likely and appropriate action.
Security+ SY0-701 recommends network segmentation for IoT and sensor devices to reduce attack surface and limit lateral movement. A dedicated VLAN isolates sensors from critical systems while allowing controlled access to data collectors or management platforms.
Adding items to a risk register (A) documents risk but does not provide protection. Physically air gapping (C) contradicts the requirement for Wi-Fi connectivity. Configuring TLS 1.2 (D) is beneficial for data-in-transit protection but does not address network-level isolation and blast-radius reduction.
Thus, B: Create a VLAN for the sensors best aligns with secure design.

NEW QUESTION: 311
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. Password policy
C. Access badges
D. Risk assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 312
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: 313
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: 314
A penetration tester is testing the security of a building's alarm system. Which type of penetration test is being conducted?
A. Physical
B. Defensive
C. Integrated
D. Continuous
Answer: (SHOW ANSWER)
Testing the security of a building's alarm system falls under physical penetration testing. According to Security+ SY0-701, physical penetration tests evaluate the effectiveness of physical security controls such as locks, alarms, cameras, sensors, badge readers, and access control points. These tests simulate real-world attempts to bypass or disable physical protections.
Defensive testing (B) refers to defensive security operations, not pen testing scope. Integrated testing (C) relates to combined system evaluations but is not a standard pen testing category. Continuous testing (D) refers to ongoing automated tests, not physical alarm evaluation. Thus, the correct answer is A: Physical.

NEW QUESTION: 315
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: B (LEAVE A REPLY)
The correct answer is Wired because Network Access Control (NAC) platforms are primarily designed to control and secure access to an organization's wired and wireless network infrastructure, with a strong emphasis on enforcing policies at the point where devices connect to the network. In the context of the Security+ SY0-701 objectives, NAC is a key architectural control used to reduce attack surface by preventing unauthorized, unmanaged, or noncompliant devices from gaining network access.
A NAC solution works by authenticating and evaluating devices before granting them access to network resources. This commonly includes checking device identity, credentials, patch levels, antivirus status, and compliance with security policies. For wired networks, NAC enforces controls at switch ports using technologies such as 802.1X, ensuring that only approved devices can connect to internal networks. This directly protects the wired attack surface by stopping threats like rogue devices, compromised laptops, or unauthorized systems from plugging into an Ethernet port and gaining access.
Option A, Bluetooth, is incorrect because NAC platforms do not directly manage short-range personal area network technologies. Option C, NFC, is also incorrect because NFC is typically used for proximity-based authentication or payments and is outside the scope of NAC enforcement. Option D, SCADA, refers to industrial control systems, which require specialized security controls and are not the primary target of standard enterprise NAC solutions.
The SY0-701 study guide highlights NAC as a preventive and detective control that supports zero trust principles by verifying devices before allowing access. By securing the wired network attack surface, NAC significantly reduces lateral movement opportunities and limits the impact of compromised or unauthorized endpoints following a security incident.

NEW QUESTION: 316
As part of new compliance audit requirements, multiple servers need to be segmented on different networks and should be reachable only from authorized internal systems. Which of the following would meet the requirements?
A. Configure firewall rules to block external access to Internal resources.
B. Set up a WAP to allow internal access from public networks.
C. Implement a new IPSec tunnel from internal resources.
D. Deploy an Internal Jump server to access resources.
Answer: A (LEAVE A REPLY)
"Network segmentation is a security practice that divides a network into smaller, isolated segments to limit access and reduce the attack surface. Firewalls are commonly used to enforce segmentation by creating rules that allow or deny traffic based on source, destination, and port. Tomeet compliance requirements, such as restricting access to internal servers, firewall rules can be configured to block all external traffic while permitting only authorized internal systems to communicate with the segmented servers. This ensures that sensitive resources are isolated from unauthorized access." Reference:CompTIA Security+ SY0-701 Study Guide, Domain 2.0: Architecture and Design, Section:
"Secure Network Architecture Concepts" (Firewalls and network segmentation are key topics).
Explanation:The requirement is to segment servers on different networks and restrict access to only authorized internal systems. Option A directly addresses this by using firewall rules to block external access while allowing internal traffic, aligning with network segmentation best practices. Option B (WAP) refers to a Wireless Access Point, which doesn't fit the context of segmentation and could expose resources to public networks. Option C (IPSec tunnel) secures communication but doesn't inherently segment networks. Option D (jump server) adds a layer of access control but doesn't address the segmentation requirement alone. Thus, A is the best fit.

NEW QUESTION: 317
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: 318
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: B (LEAVE A REPLY)
ACertificate Revocation List (CRL)is adigitally signed list maintained by a Certificate Authority (CA)that containsrevoked or expired certificates. This prevents clients from trustingcompromised 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.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

NEW QUESTION: 319
Which of the following should be used to ensure that a device is inaccessible to a network-connected resource?
A. Disablement of unused services
B. Web application firewall
C. Host isolation
D. Network-based IDS
Answer: C (LEAVE A REPLY)
Host isolation ensures that a device cannot communicate with other systems on the network. Isolation is typically applied through EDR/XDR tools, quarantine mechanisms, or endpoint firewalls. Security+ SY0-701 identifies host isolation as a containment technique used when:
A device is suspected of compromise
Lateral movement must be prevented
Sensitive systems must be protected
A system must be completely cut off except for administrative access
Isolation enforces an immediate block on all inbound and outbound communications, effectively making the device inaccessible to any network-based resource.
Disablement of unused services (A) reduces attack surface but does not isolate the device.
A WAF (B) protects web applications, not device access.
A network IDS (D) only monitors traffic and does not block access.
Thus, C: Host isolation is the correct answer.

NEW QUESTION: 320
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: 321
A security analyst is reviewing the security of a SaaS application that the company intends to purchase.
Which of the following documentations should the security analyst request from the SaaS application vendor?
A. Service-level agreement
B. Third-party audit
C. Statement of work
D. Data privacy agreement
Answer: B (LEAVE A REPLY)
A third-party audit provides an independent assessment of the SaaS vendor's security controls, compliance, and practices. This documentation helps verify that the vendor meets security standards and follows best practices.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.3: "Third-party audits offer independent verification of vendor security controls."
Exam Objectives 5.3: "Summarize third-party risk management concepts."

NEW QUESTION: 322
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: 323
A security team purchases a tool for cloud security posture management. The team is quickly overwhelmed by the number of misconfigurations that the tool detects. Which of the following should the security team configure to establish workflows for cloud resource security?
A. CASB
B. IAM
C. SOAR

D. XDR
Answer: C (LEAVE A REPLY)
SOAR (Security Orchestration, Automation, and Response) platforms enable security teams to automate workflows, prioritize alerts, and manage remediation activities, helping to handle the volume of cloud misconfiguration alerts efficiently.
CASB (A) provides visibility and control for cloud services but is less focused on orchestration. IAM (B) manages identities and permissions, and XDR (D) is extended detection but does not provide workflow automation.
SOAR integration is critical for cloud security operations discussed in Security Operations#6:Chapter
14 CompTIA Security+ Study Guide#.

NEW QUESTION: 324
Which of the following tools is best for logging and monitoring in a cloud environment?
A. IPS
B. NAC
C. FIM
D. SIEM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 325
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