CompTIA.SY0-701.v2026-11-12.q407

Exam Code:	SY0-701
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	407
Version:	v2026-11-12
# of views:	104
# of Questions views:	4072
https://www.freecram.net/torrent/CompTIA.SY0-701.v2026-11-12.q407.html	

NEW QUESTION: 1
Which of the following is a vulnerability concern for end-of-life hardware?
A. Failure to follow hardware disposal procedures could result in unintended data release.
B. The supply chain may not have replacement hardware.
C. Newly released software may require computing resources not available on legacy hardware.
D. The vendor may stop providing patches and updates.
Answer: (SHOW ANSWER)
The most significant vulnerability concern for end-of-life (EOL) hardware is that vendors stop providing patches and updates. CompTIA Security+ SY0-701 highlights that unsupported hardware and software no longer receive security fixes, leaving known vulnerabilities permanently unpatched. This creates an expanding attack surface that adversaries can easily exploit.
Once hardware reaches EOL status, newly discovered vulnerabilities will remain unaddressed, increasing the likelihood of compromise. This is especially dangerous for systems exposed to networks or handling sensitive data, where exploitation can lead to data breaches, lateral movement, or service disruption.
Option A relates to disposal risks, not active vulnerabilities. Option B is a logistical issue, not a security vulnerability. Option C is a compatibility concern, not a direct vulnerability.
Because unpatched systems are inherently vulnerable and cannot be secured through updates, the correct answer is D: The vendor may stop providing patches and updates.

NEW QUESTION: 2
After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?
A. Compensating
B. Detective
C. Preventive
D. Corrective
Answer: (SHOW ANSWER)

Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.
Reference:
Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance." CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Detective controls are designed to identify and monitor any malicious activity or anomalies on a system or network." Control Types - CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ..., under "Detective Controls": "Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network."

NEW QUESTION: 3
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.
Reference = 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: 4
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: (SHOW ANSWER)
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.

NEW QUESTION: 5
The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?
A. Fines
B. Reputational damage
C. Sanctions
D. Contractual implications
Answer: (SHOW ANSWER)
The most direct and immediate consequence of non-compliance with local data privacy regulations is fines. CompTIA Security+ SY0-701 emphasizes that privacy and data protection laws (such as GDPR, HIPAA, or regional privacy statutes) include explicit financial penalties for organizations that fail to meet compliance requirements. These fines are measurable, enforceable, and frequently cited by regulators as primary enforcement mechanisms.
While reputational damage (B) and contractual implications (D) are serious secondary effects, they are indirect and harder to quantify. Sanctions (C) typically apply in geopolitical or trade contexts rather than routine privacy enforcement. Boards of directors are often most responsive to clearly defined financial exposure; fines provide a concrete, defensible rationale for allocating additional budget to compliance, tooling, staffing, and process improvements.
Security+ SY0-701 highlights risk communication to executives using quantifiable impacts. Presenting the likelihood and magnitude of regulatory fines directly supports a cost-benefit analysis and demonstrates fiduciary responsibility. Therefore, A: Fines is the most appropriate consequence to present.

NEW QUESTION: 6
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: (SHOW ANSWER)
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.
Reference =
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: 7
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: 8
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: (SHOW ANSWER)

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: 9
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. DLP software
B. DNS filtering
C. Guardralls
D. Antivirus signatures
E. Stateful firewall
F. File integrity monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following agreements defines response time, escalation points, and performance metrics?
A. BPA
B. MOA
C. NDA
D. SLA
Answer: (SHOW ANSWER)
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: 11
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: (SHOW ANSWER)
Detailed 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: 12
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: 13
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?
A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading
Answer: D (LEAVE A REPLY)
Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. Reference = Sideloading - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

NEW QUESTION: 14
A security analyst collects IOCs from a cybersecurity bulletin. Which of the following should the analyst do next to assess if an environment is compromised?
A. Root cause analysis
B. Threat hunting
C. Tabletop exercise
D. Penetration test
Answer: (SHOW ANSWER)

Threat hunting is the correct next step because the analyst already has indicators of compromise from a cybersecurity bulletin and now needs to search the environment for evidence of those indicators. Threat hunting is proactive investigation using IOCs, threat intelligence, logs, endpoint telemetry, network data, and SIEM queries to determine whether malicious activity exists. Root cause analysis happens after an incident is confirmed and understood. A tabletop exercise is a simulated discussion used to test response readiness, not to check current compromise. A penetration test is an authorized offensive assessment and does not directly use received IOCs to determine whether systems are already affected. Security+ treats IOC-driven investigation as a threat hunting activity.

NEW QUESTION: 15
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. IDS
B. Application
C. Antivirus
D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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. Simulated threats
B. Insider threat detection
C. Business continuity planning
D. Phishing awareness
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
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: 18
Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?
A. Physical
B. Managerial
C. Technical
D. Operational
Answer: (SHOW ANSWER)
A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors. Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

NEW QUESTION: 19
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.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

NEW QUESTION: 20

A security engineer receives reports of unauthorized devices on the organization's network. Which of the following best describes a secure and effective way to mitigate the risks?

Freectam.net

A. Deploy a NAC solution to block wireless connections until devices can be verified against the baseline configuration.
B. Set the NAC solution to only accept handshakes initiated from a static set of IP addresses.
C. Configure a NAC solution to enforce 802.1X authentication with device certificates and implement endpoint security checks.
D. Implement a NAC solution that redirects all devices to the guest Wi-Fi for holding until a security analyst can validate the security compliance.
Answer: (SHOW ANSWER)
The best answer is C. Configure a NAC solution to enforce 802.1X authentication with device certificates and implement endpoint security checks.
NAC (Network Access Control) is used to verify devices before granting them access to the network. A strong NAC deployment should validate both identity and security posture. Enforcing 802.1X authentication ensures that devices must authenticate before connecting, and using device certificates strengthens trust in the device itself. Endpoint security checks add posture assessment, such as confirming antivirus, patch level, or compliance state.
This is the most secure and effective approach because it prevents unauthorized or noncompliant devices from joining the network in the first place.
Why the other options are incorrect:
A . Deploy a NAC solution to block wireless connections until devices can be verified against the baseline configuration.This only addresses wireless access and is too limited. Unauthorized devices could still attempt access in other ways.
B . Set the NAC solution to only accept handshakes initiated from a static set of IP addresses.IP addresses are not a reliable basis for device trust and can be spoofed or reassigned.
D . Implement a NAC solution that redirects all devices to the guest Wi-Fi for holding until a security analyst can validate the security compliance.Redirecting all devices is not practical or efficient, and guest Wi-Fi is not the best control for secure admission.
From a Security+ perspective, the strongest NAC implementation uses 802.1X, certificates, and posture assessment, making C correct.

NEW QUESTION: 21
Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).
A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor
Answer: (SHOW ANSWER)

Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

NEW QUESTION: 22
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.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of physical security and access control.

NEW QUESTION: 23
An administrator discovers a cross-site scripting vulnerability on a company website. Which of the following will most likely remediate the issue?
A. Input validation
B. NGFW
C. Vulnerability scan
D. WAF
Answer: (SHOW ANSWER)
Cross-site scripting (XSS) occurs when a web application fails to properly validate or sanitize user input, allowing attackers to inject malicious scripts into web pages viewed by other users. The most effective remediation is input validation, which ensures that only safe, expected data is accepted by the application.
Security+ SY0-701 highlights input validation as a primary defense against:
* XSS
* SQL injection
* Command injection
* Path traversal attacks
By validating and sanitizing input at both the client and server layers, organizations can strip harmful characters, block script tags, enforce strict data types, and ensure proper encoding.
A NGFW (B) or WAF (D) can mitigate attacks by blocking malicious payloads, but they do not fix the root cause within the web application. A vulnerability scan (C) identifies the issue but does not remediate it.
Therefore, only input validation (A) directly resolves the underlying coding flaw responsible for XSS.

NEW QUESTION: 24
The security team notices that the Always On VPN solution sometimes fails to connect. This leaves remote users unprotected because they cannot connect to the on-premises web proxy. Which of the following changes will best provide web protection in this scenario?
A. Implement network access control.
B. Configure the local gateway to point to the VPN.
C. Create a public NAT to the on-premises proxy.
D. Install a host-based content filtering solution.
Answer: (SHOW ANSWER)
Installing a host-based content filtering solution on the endpoints ensures that web traffic is filtered locally even when the VPN connection to the on-premises proxy fails, maintaining protection for remote users.
Network access control (A) manages device network access, local gateway configuration (B) does not solve protection if VPN fails, and public NAT (C) exposes internal resources and increases risk.
Endpoint filtering complements VPN for resilient web security, covered in Security Architecture and Operations#6:Chapter 11 CompTIA Security+ Study Guide#.

NEW QUESTION: 25
Which of the following can be used to mitigate attacks from high-risk regions?
A. IP geolocation
B. Encryption
C. Data sovereignty
D. Obfuscation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
A legal department must maintain a backup from all devices that have been shredded and recycled by a third party. Which of the following best describes this requirement?
A. Data retention
B. Destruction
C. Sanitation
D. Certification
Answer: A (LEAVE A REPLY)

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. Validating the accuracy of the evidence collected during the investigation
C. Determining the root cause of the incident
D. Developing steps to mitigate the risks of the incident
Answer: (SHOW ANSWER)

NEW QUESTION: 28

Which of the following describes how a risk event might affect operations and limit the overall risk score?

A. Severity

B. Likelihood

C. Impact

D. Probability

Answer: (SHOW ANSWER)

Severity describes how serious a risk event would be if it occurred and is commonly used to prioritize remediation. In practical risk management, severity reflects the operational consequence of an event, such as service disruption, data loss, regulatory exposure, financial damage, or safety concerns. Likelihood and probability both describe the chance that the event will occur, not the seriousness of the result. Impact is closely related, but severity is the scoring label often used to express the overall seriousness of the risk in a risk register, vulnerability report, or risk matrix. For Security+, severity helps determine which risks require immediate treatment and which can be accepted, monitored, or deferred.

NEW QUESTION: 29

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

A. Analysis

B. Lessons learned

C. Detection

D. Containment

Answer: (SHOW ANSWER)

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned. Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

NEW QUESTION: 30

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?

Freecram.net

A. Race condition

B. Memory injection

C. Malicious update

D. Side loading

Answer: (SHOW ANSWER)

A race condition occurs when two 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 field before the SQL update completed, indicating a time-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 is not what 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.

NEW QUESTION: 31
Which of the following should be used to aggregate log data in order to create alerts and detect anomalous activity?
A. SIEM
B. WAF
C. Network taps
D. IDS
Answer: (SHOW ANSWER)
A Security Information and Event Management (SIEM) solution collects, aggregates, and correlates logs from multiple sources to detect anomalies and generate alerts. SIEMs are essential for security monitoring and incident detection.Reference: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
Which of the following is a qualitative approach to risk analysis?
A. Including the MTTR and MTBF as part of the risk assessment
B. Tracking and documenting network risks using a risk register
C. Assigning a level of high, medium, or low to the risk rating
D. Using ALE and ARO to help determine whether a risk should be mitigated
Answer: (SHOW ANSWER)
A qualitative risk analysis assigns descriptive ratings such as high, medium, or low to risks based on their likelihood and impact without numerical calculations.
Including MTTR/MTBF (A) and ALE/ARO (D) are quantitative methods using metrics. Risk registers (B) document risks but don't specify analysis type. Qualitative and quantitative risk methods are fundamental in SY0-701 risk management [6:Chapter 17 CompTIA Security+ Study Guide].

NEW QUESTION: 33
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 device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test1.

NEW QUESTION: 34
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: (SHOW ANSWER)
PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.
If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.
The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment. B. Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls and recommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non-compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors. Reference = 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: 35
Which of the following cryptographic solutions protects data at rest?
A. Full disk encryption
B. Digital signatures
C. Private key
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 36
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?
A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
Answer: (SHOW ANSWER)
A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:
Access list <direction> <action> <source address> <destination address> <protocol> <port> To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.

NEW QUESTION: 37
An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?
A. Zero-day attacks
B. Insider threats
C. End-of-life support
D. Known exploits
Answer: (SHOW ANSWER)

Applying the latest OS updates, patches, and endpoint definitions is the most effective way to prevent known exploits, which are attacks leveraging previously discovered vulnerabilities for which fixes are available.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Applying patches and updates prevents exploitation of known vulnerabilities." Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

NEW QUESTION: 38
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 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: 39
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. Reference = 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: 40
For which of the following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?
Freecram.net
A. To validate the authenticity of the file
B. To calculate the checksum of the file
C. To activate the license for the file
D. To test the integrity of the file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41

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: (SHOW ANSWER)

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: 42

SIMULATION

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

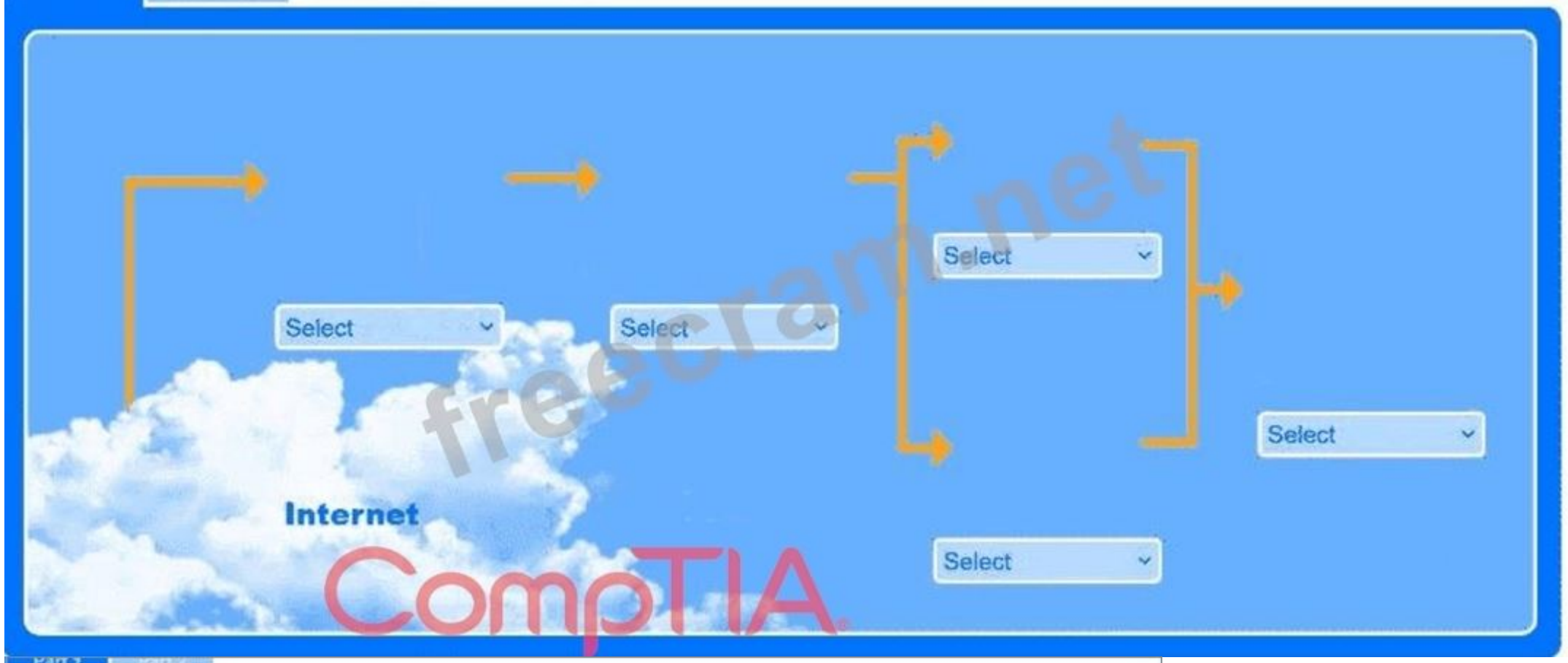
Part 1

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



freecram.net
CompTIA

Part 1 Part 2



freecram.net
CompTIA

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)
```

freecram.net

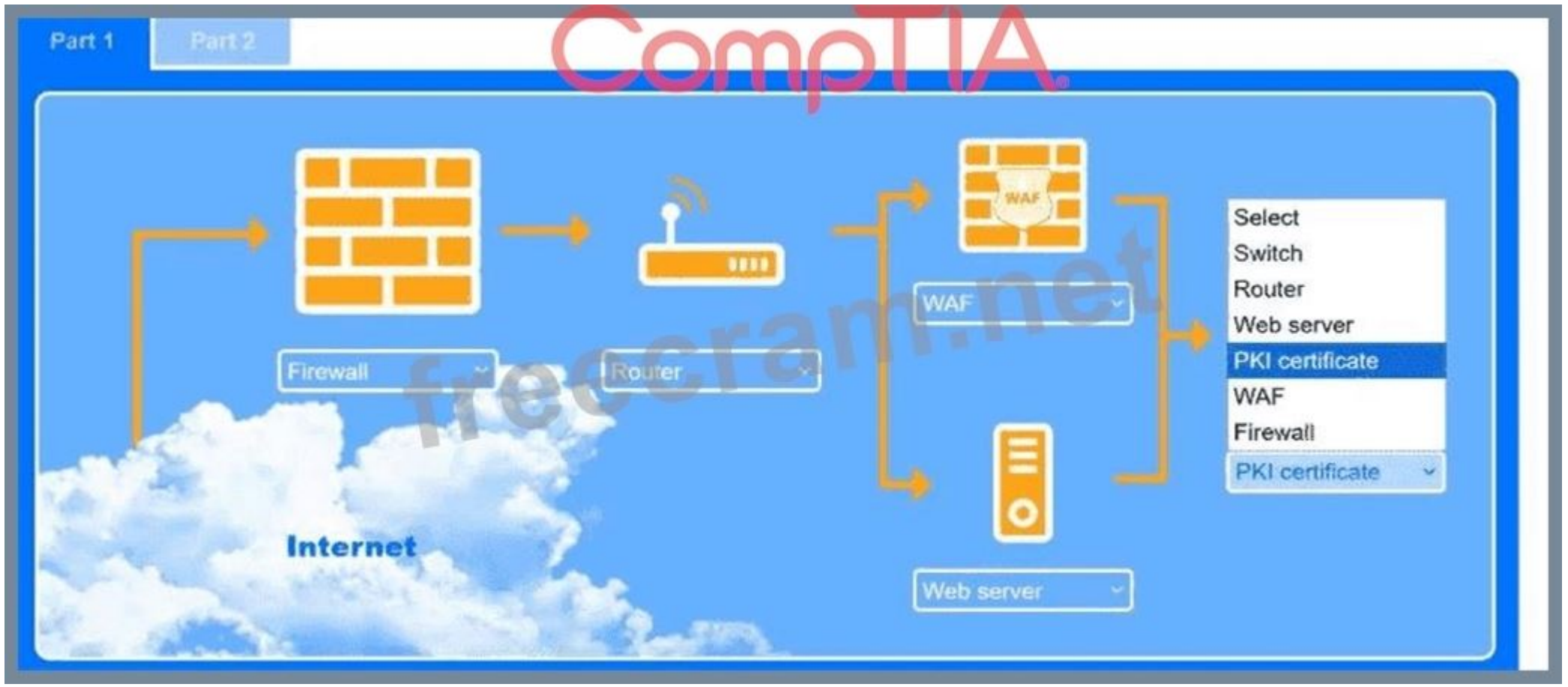
CompTIA



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

CompTIA
freecram.net

NEW QUESTION: 43
A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?
A. Tolerance
B. Appetite
C. Threshold
D. Register
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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: (SHOW ANSWER)
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.Reference: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 45
Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?
A. Client
B. Third-party vendor
C. Cloud provider
D. DBA
Answer: A (LEAVE A REPLY)
According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on

the cloud infrastructure. Therefore, the client is responsible for securing the company's database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security. Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 263-264; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

NEW QUESTION: 46
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: (SHOW ANSWER)
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#

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 47
A security analyst is monitoring logs from the organization's SIEM and identifies logs related to one of their salespeople:
Time | IP address | Location | EmpID | App | Status
14:02 | 72.45.38.27 | Atlanta | 25687 | VPN | Success
14:04 | 72.45.38.27 | Atlanta | 25687 | Email | Failure
14:07 | 58.67.47.48 | Beijing | 25687 | VPN | Success
14:15 | 72.45.38.27 | Atlanta | 25687 | Teams | Success
Which of the following is being displayed in the logs?
A. Impossible travel
B. SMTP replay
C. Directory traversal
D. Cross-site request forgery
Answer: (SHOW ANSWER)

The logs show impossible travel because the same employee account is successfully authenticating from Atlanta and Beijing within minutes. A legitimate user cannot physically travel between those locations in that short period of time. In Security+ operations, impossible travel is an identity and access anomaly often detected by SIEM, IAM, CASB, or UEBA tools. It may indicate credential theft, session hijacking, VPN abuse, or malicious login activity. SMTP replay relates to email transmission or abuse and does not explain geographically impossible logins. Directory traversal is a web attack that attempts to access unauthorized file paths. Cross-site request forgery tricks an authenticated browser into submitting unwanted requests. The location and timing pattern clearly indicates impossible travel.

NEW QUESTION: 48
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: (SHOW ANSWER)
Detailed 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: 49
A company relies on open-source software libraries to build the software used by its customers. Which of the following vulnerability types would be the most difficult to remediate due to the company's reliance on open- source libraries?
A. Buffer overflow
B. SQL injection
C. Cross-site scripting
D. Zero day
Answer: (SHOW ANSWER)
Zero-day vulnerabilities are unknown flaws in software, making them harder to patch, especially when using open-source libraries without dedicated support teams.

NEW QUESTION: 50
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?
Freecram.net
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: (SHOW ANSWER)
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. Reference = 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: 51
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 rapidlyanalyzes host and network data from potentially compromised systems and forwards the data for further review. Which of the following tools should the incident response team deploy?
A. NAC
B. IPS
C. SIEM
D. EDR
Answer: (SHOW ANSWER)
AnEndpoint Detection and Response (EDR)solution is designed tomonitor, detect, and respond to security incidents on endpoints (such as workstations and servers). Itcollects 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 choicefor analyzing and responding to endpoint security incidents.

NEW QUESTION: 52
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: B (LEAVE A REPLY)
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

NEW QUESTION: 53
A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?

A. Threshold
B. Appetite
C. Avoidance
D. Register
Answer: B (LEAVE A REPLY)
Risk appetiterefers to thelevel of risk an organization is willing to acceptbefore implementing security measures. When expanding access controls, the company must assess how much risk is acceptable in terms of data exposure, unauthorized access, and compliance obligations.

NEW QUESTION: 54
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: (SHOW ANSWER)
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."

NEW QUESTION: 55
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: 56
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: (SHOW ANSWER)
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.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptographic Techniques.

NEW QUESTION: 57
Which of the following is an example of a certificate that is generated by an internal source?
A. Digital signature
B. Asymmetric key
C. Self-signed
D. Symmetric key
Answer: (SHOW ANSWER)
A self-signed certificate is generated internally without involving an external Certificate Authority (CA). In a self-signed certificate, the certificate issuer and certificate subject are the same entity. Security+ SY0-701 explains that organizations frequently use self-signed certificates for internal systems, lab environments, or testing scenarios where external trust chains are unnecessary.
A digital signature (A) is a cryptographic function, not a certificate. Asymmetric keys (B) are used in public- key cryptography but do not constitute a certificate by themselves. Symmetric keys (D) are encryption tools, not certificates.
Therefore, the example of a certificate generated internally is C: Self-signed.

NEW QUESTION: 58
A penetration tester must conduct a vulnerability assessment on a target network to identify potential security weaknesses. Which of the following tools will best achieve this goal?
A. Metasploit
B. Burp Suite
C. Nessus
D. Wireshark

Answer: (SHOW ANSWER)
Nessus is the best answer because it is a dedicated vulnerability assessment scanner. Its purpose is to scan systems, services, ports, configurations, missing patches, weak protocols, and known CVEs, then produce a report of discovered weaknesses. That directly matches the requirement to "identify potential security weaknesses" on a target network. Metasploit is mainly an exploitation framework used to validate or exploit vulnerabilities, not the best first-choice vulnerability assessment tool. Burp Suite is primarily used for web application testing, not broad network vulnerability assessment. Wireshark captures and analyzes packets, which is useful for troubleshooting and traffic inspection but does not perform vulnerability assessment. For Security+, Nessus maps clearly to vulnerability scanning and assessment.

NEW QUESTION: 59
A security administrator needs to protect the integrity of a compromised laptop. The administrator turns off the laptop for a forensic investigation. Which of the following tasks should the administrator do first before analyzing the hard drive?
A. Metadata review
B. Snapshot
C. Bit-level copy
D. Memory dump
Answer: (SHOW ANSWER)
The administrator should create a bit-level copy before analyzing the hard drive. In digital forensics, original evidence must be preserved in its exact state to maintain integrity and support chain of custody. A bit-level copy, also called a forensic image, captures every sector of the drive, including deleted data, slack space, and hidden artifacts. Analysis should then be performed on the copy, not the original evidence. A metadata review is useful later but should not happen before evidence preservation. A snapshot usually applies to virtual machines or system states, not a powered-off physical laptop drive. A memory dump would normally be collected before shutdown because RAM is volatile, but the laptop has already been turned off.

NEW QUESTION: 60
Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?
Freecram.net
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. Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors - CompTIA Security+ SY0-701 - 2.1, video by Professor Messer.

NEW QUESTION: 61
An administrator wants to automate an account permissions update for a large number of accounts. Which of the following would best accomplish this task?
A. Security groups
B. Vertical scaling
C. Federation

D. User provisioning
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 62
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: 63
A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.
Most employees clocked in and out while they were Inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while Inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.
Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet. Which of the following Is the most likely reason for this compromise?
A. A brute-force attack was used against the time-keeping website to scan for common passwords.
B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.
C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site
D. ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.machine.
Answer: (SHOW ANSWER)
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.

Reference =
CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

NEW QUESTION: 64
An analyst identifies that multiple users have the same passwords, but the hashes appear to be completely different. Which of the following most likely explains this issue?
A. Data masking
B. Salting
C. Key escrow
D. Tokenization
Answer: (SHOW ANSWER)
Salting involves adding a unique value (salt) to each password before hashing it. This means that even if two users have the same password, the added salts ensure their hash values are different. This protects against attacks that exploit identical hash values, such as rainbow table attacks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Salting passwords ensures that identical passwords do not have identical hashes, even if the same hash algorithm is used." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 65
Which of the following is a prerequisite for a DLP solution?
A. Data destruction
B. Data sanitization
C. Data classification
D. Data masking
Answer: (SHOW ANSWER)
Data classification is required before implementing a Data Loss Prevention (DLP) solution because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.
Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.
Data classification is emphasized in Security Program Management and Data Protection topics [6:Chapter 16 CompTIA Security+ Study Guide].

NEW QUESTION: 66
A company asks a vendor to help its internal red team with a penetration test without providing too much detail about the infrastructure. Which of the following penetration testing methods does this scenario describe?
A. Passive reconnaissance
B. Partially-known environment
C. Integrated testing
D. Defensive testing
Answer: (SHOW ANSWER)
This scenario describes a partially-known environment penetration test. In CompTIA Security+ SY0-701, penetration testing approaches are commonly categorized as black box (unknown), white box (fully known), and gray box (partially known). A partially-known environment means the tester is given limited information-enough to be realistic and efficient, but not complete details about the infrastructure.

Here, the vendor is assisting an internal red team and is intentionally not provided with extensive infrastructure details, which mirrors a gray-box testing approach. This method balances realism and efficiency by simulating an attacker who has some knowledge (such as credentials, architecture diagrams, or application details) but not full access or documentation.
Passive reconnaissance (A) is an activity within testing, not a testing methodology. Integrated testing (C) refers to coordinated testing involving multiple teams (e.g., red and blue teams) with full cooperation. Defensive testing (D) focuses on validating defensive controls rather than simulating an attacker's perspective.
Therefore, the correct answer is B: Partially-known environment.

NEW QUESTION: 67
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. Reference: 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: 68
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.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

NEW QUESTION: 69

An attacker floods an organization's VoIP phone system with thousands of requests. This causes legitimate calls to drop or fail to connect. Analysis shows the attacker faked internal extensions to trick users into answering calls and sharing sensitive information. Which of the following types of attacks has the attacker used in this incident? (Select two).

A. SIP spoofing attack
B. On-path attack
C. Packet sniffing attack
D. Vishing attack
E. Denial-of-service attack
F. Supply chain attack

Answer: (SHOW ANSWER)

The attacker used a denial-of-service attack and a vishing attack. The flood of thousands of VoIP requests causes legitimate calls to drop or fail, which is an availability attack and clearly maps to denial of service. The second behavior involves tricking users over voice communications into sharing sensitive information, which is vishing. Vishing is voice-based phishing and commonly abuses trust, urgency, caller ID manipulation, or internal-looking extensions. SIP spoofing may appear related because fake internal extensions are mentioned, but the question asks for two attack types that describe the overall incident: service disruption and voice-based social engineering. On-path attacks involve interception, packet sniffing captures traffic, and supply chain attacks compromise vendors or dependencies.

NEW QUESTION: 70

Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems
D. SCADA

Answer: B (LEAVE A REPLY)

Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION: 71

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: (SHOW ANSWER)

An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or dat a. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they 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.

NEW QUESTION: 72
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: (SHOW ANSWER)
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

NEW QUESTION: 73
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: (SHOW ANSWER)
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.
Reference:
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: 74
A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).
A. Private
B. Confidential
C. Public

D. Operational
E. Urgent
F. Restricted
Answer: (SHOW ANSWER)
Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:
Public: Data that can be freely disclosed to anyone without any harm or risk.
Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.
Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.
Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.
In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2. Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

NEW QUESTION: 75
A company is in the process of migrating to cloud-based services. The company's IT department has limited resources for migration and ongoing support. Which of the following best meets the company's needs?
A. IAM
B. SASE
C. WAF
D. IPS
Answer: (SHOW ANSWER)

NEW QUESTION: 76
An administrator must implement a solution that provides security and network connectivity between two companies. Which of the following infrastructure solutions is the best for this purpose?
A. UTM
B. VPN
C. NAC
D. NGFW
Answer: (SHOW ANSWER)
The best answer is B. VPN.
A VPN (Virtual Private Network) is the standard solution for securely connecting two separate organizations or networks across an untrusted network, such as the internet. A site-to-site VPN provides:
secure connectivity between both companies
encrypted traffic in transit
protection of data confidentiality and integrity
a practical way to interconnect business networks
Why the other options are incorrect:

A). UTMA unified threat management device offers multiple security features, but it is not specifically the best answer for secure connectivity between two companies.
C). NACNetwork Access Control regulates which devices can connect to a network, but it does not provide intercompany network connectivity.
D). NGFWA next-generation firewall improves traffic inspection and filtering, but it is not by itself the main solution for secure network connectivity between two companies.
From the SY0-701 perspective, when secure communication between separate organizations is required, VPN is the most appropriate infrastructure solution.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Which of the following best distinguishes hacktivists from insider threats?
A. Hacktivists often act based on ideological or political beliefs rather than organizational access.
B. Hacktivists are generally employed by the target organization at the time of attack.
C. Hacktivists often target organizations without prior access or internal affiliation.
D. Hacktivists are primarily motivated by personal conflicts or employment-related dissatisfaction.
Answer: (SHOW ANSWER)
The best answer is C. Hacktivists often target organizations without prior access or internal affiliation.
The clearest distinction between hacktivists and insider threats is that insider threats typically have authorized access or internal affiliation with the organization, while hacktivists usually act from the outside.
Hacktivists are often motivated by political, ideological, or social causes, but the strongest differentiator in this comparison is that they generally do not begin with legitimate internal access.
Why the other options are less correct:
A . Hacktivists often act based on ideological or political beliefs rather than organizational access.This is true about motivation, but it does not distinguish them as directly as the lack of internal access does.
B . Hacktivists are generally employed by the target organization at the time of attack.This describes insiders, not hacktivists.
D . Hacktivists are primarily motivated by personal conflicts or employment-related dissatisfaction.This is more typical of some insider threats, not hacktivists.
From the SY0-701 perspective, the strongest distinction is external targeting without prior authorized access, so C is the best answer.

NEW QUESTION: 78
A security analyst must prevent remote users from accessing malicious URLs. The sites need to be checked inline for reputation, content, or categorization. Which of the following technologies will help secure the enterprise?
A. VPN
B. SASE
C. IDS

D. SD-WAN

Answer: (SHOW ANSWER)

Secure Access Service Edge (SASE) is the technology best suited for preventing remote users from accessing malicious URLs. According to the CompTIA Security+ SY0-701 framework, SASE integrates cloud-native security capabilities such as DNS filtering, secure web gateways, CASB, and URL categorization, all delivered inline. This means every URL request from a remote user is checked in real time for reputation, content, and category before access is granted.

This solution is specifically designed for remote workforces because security enforcement happens in the cloud, regardless of user location-eliminating reliance on on-premise proxies or VPN routing. SASE also enables consistent policy application and real-time enforcement across distributed networks.

A VPN (A) only encrypts traffic; it does not perform URL reputation checks. IDS (C) detects malicious activity but does not block URL access. SD-WAN (D) optimizes WAN routing but is not focused on content filtering or URL reputation.

Therefore, SASE is the correct and most effective solution for inline URL inspection and preventing remote users from reaching malicious sites.

NEW QUESTION: 79

A security engineer configured a remote access VPN. The remote access VPN allows end users to connect to the network by using an agent that is installed on the endpoint, which establishes an encrypted tunnel. Which of the following protocols did the engineer most likely implement?

A. GRE

B. IPSec

C. SD-WAN

D. EAP

Answer: (SHOW ANSWER)

NEW QUESTION: 80

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?

Freecram.net

A. Access control list

B. Hashing

C. Input validation

D. Permission restrictions

Answer: (SHOW ANSWER)

NEW QUESTION: 81

A Chief Security Officer signs off on a request to allow inbound SMB and RDP from the internet to a single VLAN. Which of the following is the most likely explanation for this activity?

A. The company built a new file-sharing site.

B. The organization is preparing for a penetration test.

C. The security team is integrating with an SASE platform.

D. The security team created a honeynet.

Answer: (SHOW ANSWER)

Allowing risky protocols like SMB and RDP from the internet to a controlled VLAN is commonly done to create a honeynet, a deliberately vulnerable network environment used to attract attackers and study their behaviors without risking production systems.

Building a file-sharing site (A) or preparing for a pentest (B) typically wouldn't require exposing SMB and RDP broadly. SASE integration (C) focuses on cloud security access and doesn't involve opening such protocols indiscriminately.
Honeynets are described as a deception technology in the Security Architecture domain [6:Chapter 9 CompTIA Security+ Study Guide].

NEW QUESTION: 82
Which of the following objectives is best achieved by a tabletop exercise?
A. Familiarizing participants with the incident response process
B. Deciding red and blue team rules of engagement
C. Quickly determining the impact of an actual security breach
D. Conducting multiple security investigations in parallel
Answer: (SHOW ANSWER)
A tabletop exercise is a discussion-based simulation where incident response (IR) team members walk through hypothetical security scenarios to understand roles, responsibilities, escalation paths, and communication processes. According to Security+ SY0-701, tabletop exercises are ideal for familiarizing participants with the incident response process and improving organizational readiness without the pressure or resource demands of full-scale simulations.
These exercises highlight:
* IR workflow clarity
* Decision-making processes
* Coordination between technical and non-technical teams
* Communication procedures
* Identification of gaps in policies or documentation
Option B (rules of engagement) is part of penetration testing planning, not tabletop exercises. Option C refers to real breach analysis, not simulations. Option D refers to forensic operations, not tabletop objectives.
Thus, A is correct.

NEW QUESTION: 83
A security analyst is prioritizing vulnerability scan results using a risk-based approach. Which of the following is the most efficient resource for the analyst to use?
A. Business impact analysis
B. Common Vulnerability Scoring System
C. Risk register
D. Exposure factor
Answer: (SHOW ANSWER)
TheCommon Vulnerability Scoring System (CVSS)is astandardized framework for assessing the severity of vulnerabilities. It provides a numerical score (0-10) based on factors such asexploitability, impact, and complexity, helping security analystsprioritize remediation efforts based on risk.
* Business impact analysis (A)helps identifycritical business functionsbut does not specifically prioritize vulnerabilities.
* Risk register (C)tracks identified risks but does not classify vulnerabilities.
* Exposure factor (D)is used inquantitative risk assessmentbut is not an industry standard for vulnerability prioritization.

NEW QUESTION: 84

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A. Mitigate

B. Accept

C. Transfer

D. Avoid

Answer: (SHOW ANSWER)

Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process. These strategies may not be feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation2

NEW QUESTION: 85

A software developer released a new application and is distributing the application files through 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)

The correct answer is A. Hashes.

A hash is a fixed-length value generated from data using a hashing algorithm. Developers often publish cryptographic hashes, such as SHA-256 hashes, so users can compare the published hash with the hash of the downloaded file. If the values match, the user has assurance that the file was not altered or corrupted after the hash was generated.

This aligns with CompTIA Security+ SY0-701 topics related to integrity, cryptographic concepts, and secure software distribution.

Why the other options are incorrect:

B . Certificates

Certificates are used to verify identity, support encryption, and enable trust in public key infrastructure. They may support code signing, but simply posting a certificate is not the standard method for users to manually verify file integrity.

C . Algorithms

Algorithms define the mathematical process used for hashing or encryption, but posting an algorithm alone does not allow users to verify a specific file's integrity.

D . Salting

Salting is commonly used with password hashing to defend against precomputed hash attacks, such as rainbow table attacks. It is not used for verifying downloaded file integrity.

Therefore, the developer should post hashes for the downloadable files.

NEW QUESTION: 86
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: 87
A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?
A. Exemption
B. Exception
C. Avoid
D. Transfer
Answer: (SHOW ANSWER)
Detailed Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Risk Management Strategies".

NEW QUESTION: 88
Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A. Destruction
B. Certification
C. Retention
D. Sanitization
Answer: C (LEAVE A REPLY)
Detailed
Retention policies dictate how long data must be stored to comply with local and international regulations. Non-compliance can result in legal and financial penalties. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Retention and Legal Requirements".

NEW QUESTION: 89
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?
A. Scalability
B. Availability
C. Cost

D. Ease of deployment

Answer: (SHOW ANSWER)

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

NEW QUESTION: 90

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?

Freecram.net

A. Full disk encryption

B. Network access control

C. File integrity monitoring

D. User behavior analytics

Answer: (SHOW ANSWER)

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: 91

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: (SHOW ANSWER)

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.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com

SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
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: (SHOW ANSWER)
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: 93
Which of the following cryptographic methods is preferred for securing communications with limited computing resources?
A. Elliptic curve cryptography
B. Hashing algorithm
C. Public key infrastructure
D. Symmetric encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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. Threat scope reduction
B. Security procedure evaluation
C. Policy review
D. Gap analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following should be used to ensure an attacker is unable to read the contents of a mobile device's drive if the device is lost?
A. TPM
B. ECC
C. FDE

D. HSM
Answer: (SHOW ANSWER)
Full Disk Encryption (FDE) ensures that all data on the drive is encrypted, preventing unauthorized access even if the device is lost.

NEW QUESTION: 96
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. Intrusion prevention system
B. Endpoint detection and response
C. Antivirus
D. Sandbox
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?
A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response
Answer: (SHOW ANSWER)
Detailed
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: 98
The Cruel Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells me analyst the installation must be done as quickly as possible. Which of the following courses of action should the security analyst take first?
A. Log in to the server and perform a health check on the VM.
B. Install the patch Immediately.
C. Confirm that the backup service is running.
D. Take a snapshot of the VM.
Answer: (SHOW ANSWER)
Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.
Reference = CompTIA Security+ SY0-701 study materials, focusing on change management and backup strategies.

NEW QUESTION: 99

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. MTTR

B. RTO

C. ARO

D. MTBF

Answer: (SHOW ANSWER)

The correct answer is C. ARO.

ARO stands for Annualized Rate of Occurrence. It estimates how often a specific event is expected to occur in one year. When deciding whether to keep or remove insurance coverage for a specific type of incident, such as ransomware, an organization may evaluate how likely that event is to occur annually.

This aligns with CompTIA Security+ SY0-701 risk management concepts, especially quantitative risk analysis and risk treatment decisions.

Why the other options are incorrect:

A). MTTR

Mean Time to Repair measures the average time required to restore a system or service after failure. It does not estimate how often ransomware will occur.

B). RTO

Recovery Time Objective defines the maximum acceptable time to restore a system or business process after an outage. It is important for business continuity but does not measure event frequency.

D). MTBF

Mean Time Between Failures measures the expected time between failures for a system or component. It is not typically used to evaluate ransomware insurance coverage.

Therefore, the most likely analysis element is ARO.

NEW QUESTION: 100

You are security administrator investigating a potential infection on a network.

Click on each host and firewall. Review all logs to determine which host originated the Infecton and then deny each remaining hosts clean or infected.

192.168.10.22

CompTIA

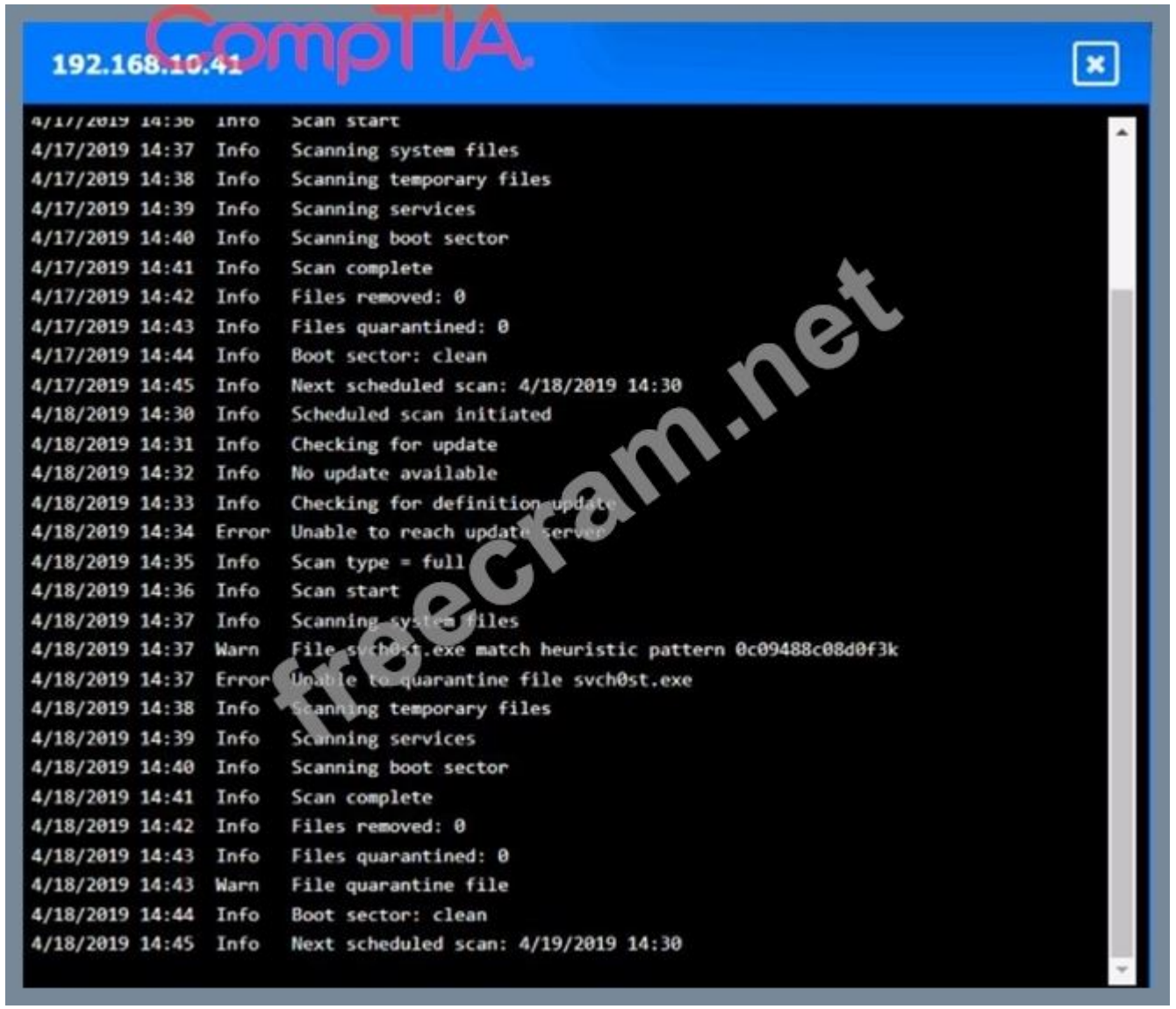
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31   Warn   Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32   Warn   Scheduled update disabled by process scvh0st.exe
```

freecram.net

192.168.10.37

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
```

CompTIA
freecram.net

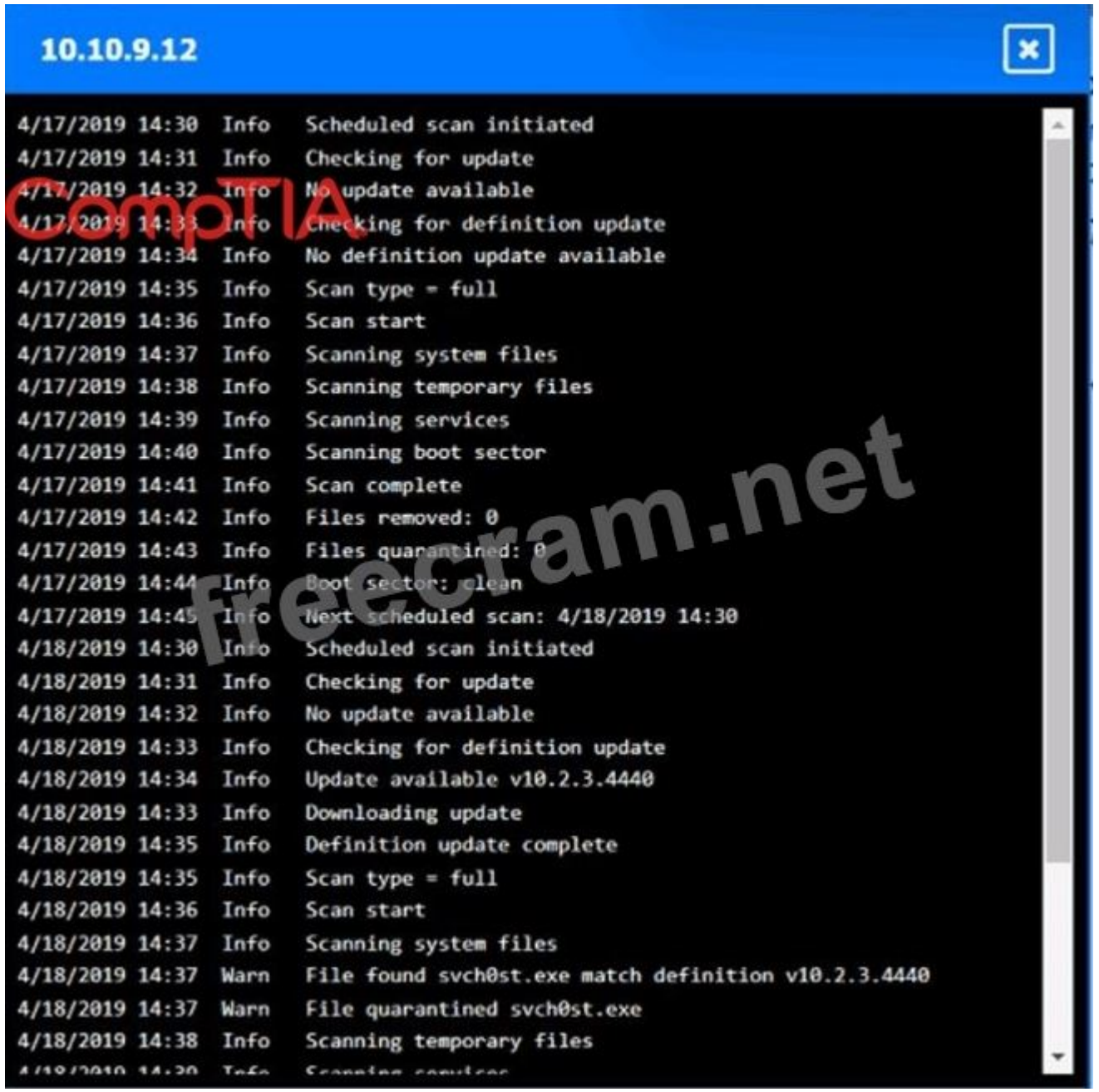


CompTIA
freecram.net

Firewall

Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

CompTIA
freecram.net

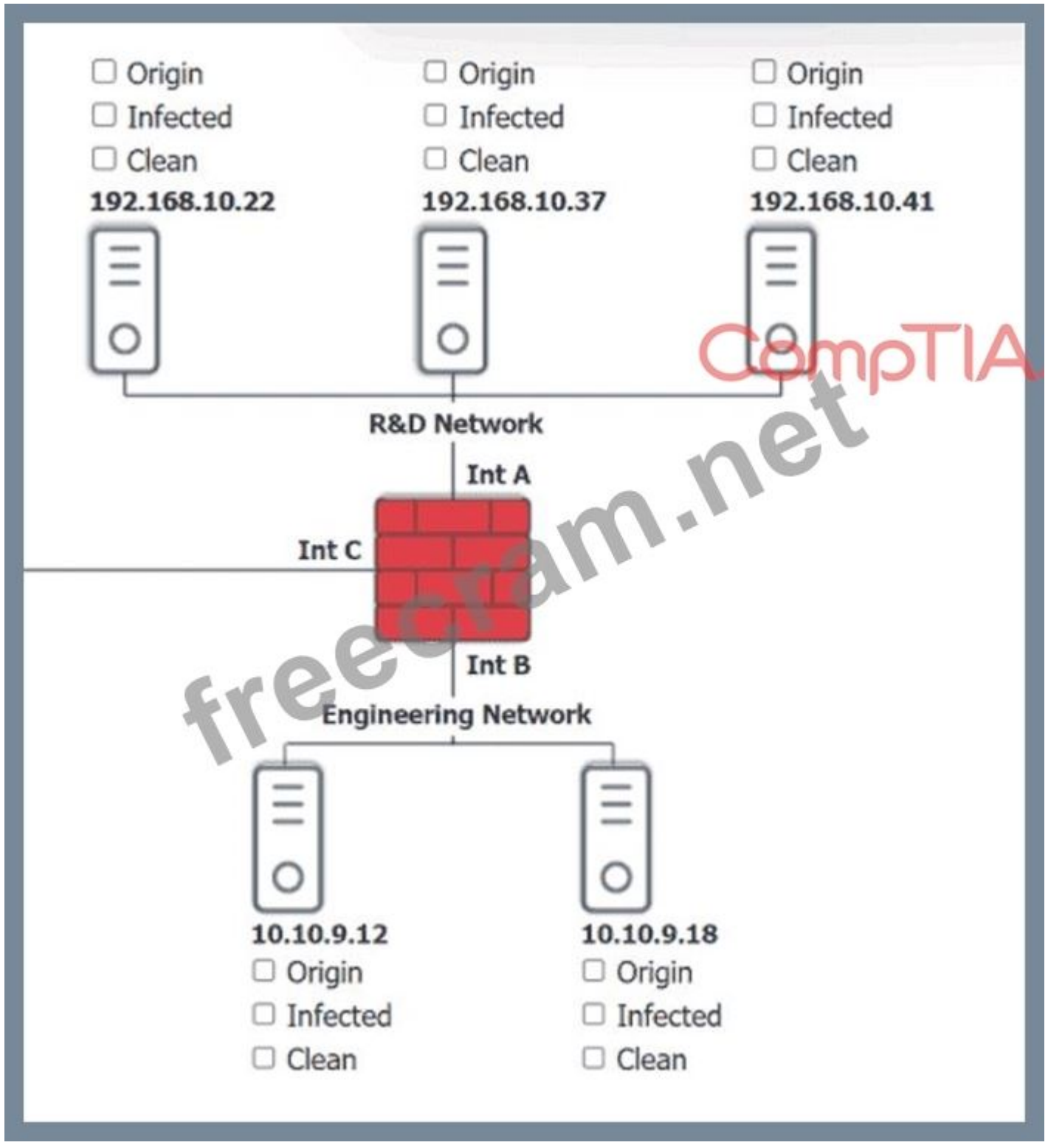


CompTIA
freecram.net

10.10.9.18

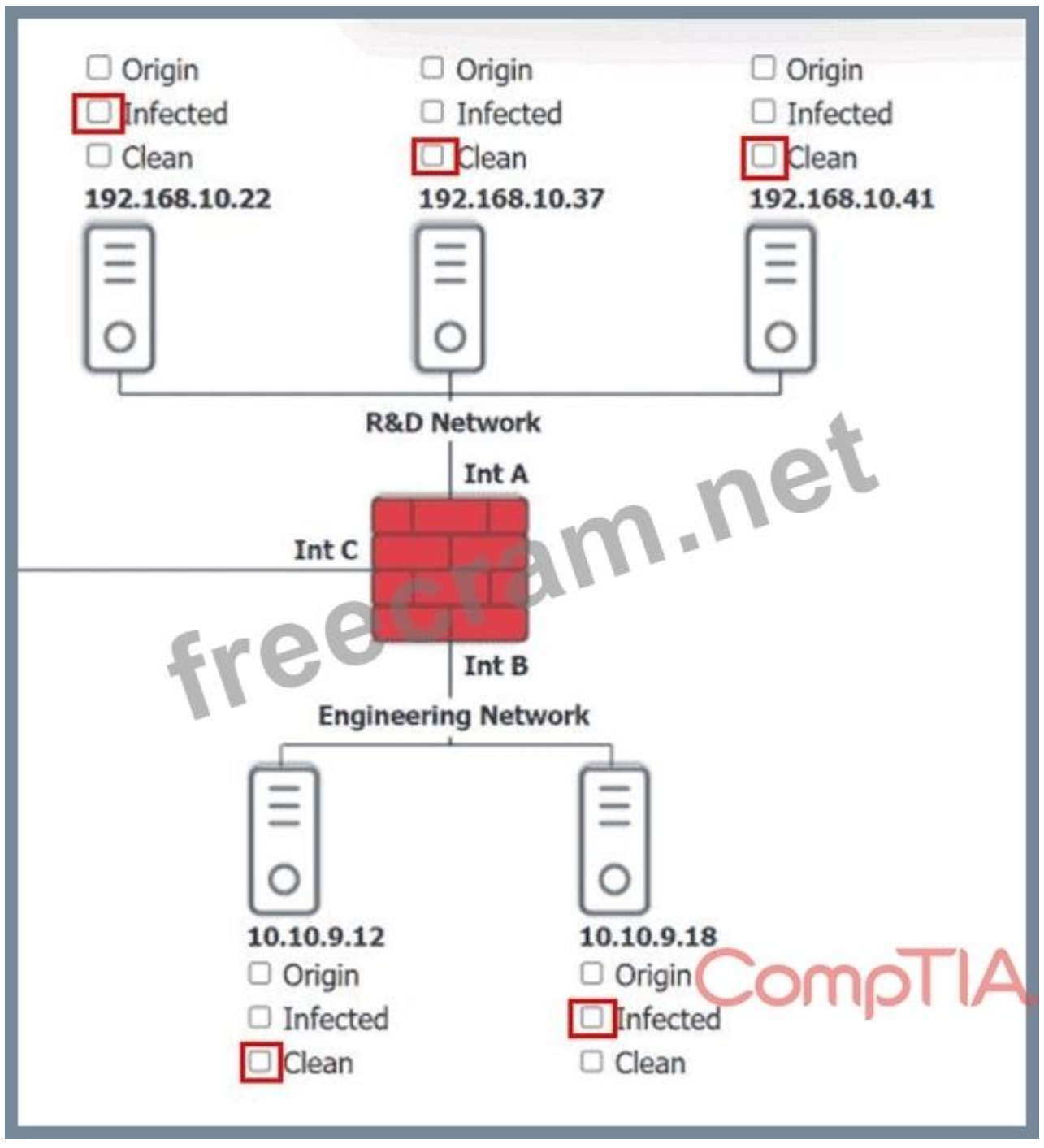
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
```

CompTIA
freecram.net



CompTIA
freecram.net

Answer:



freecram.net
CompTIA

NEW QUESTION: 101

A company uses multiple providers to send its marketing, internal, and support emails. Many of the emails are marked as spam. Which of the following changes should the company make to ensure legitimate emails are validated?

A. Disable DKIM to avoid signature conflicts.

B. Implement DMARC with a " reject " policy to enforce sender validation.

C. Replace the domain ' s MX record with the marketing provider ' s services.

D. Update the SPF record to include all authorized sending sources.

Answer: (SHOW ANSWER)

The best answer is D. Update the SPF record to include all authorized sending sources.

SPF (Sender Policy Framework) is used to identify which mail servers and third-party services are authorized to send email on behalf of a domain. In this scenario, the company uses multiple providers for marketing, internal, and support emails. If all of those sending sources are not properly listed in the domain's SPF record, receiving mail servers may treat some valid messages as suspicious or spam.
Updating the SPF record to include all legitimate sending providers helps recipient systems validate that the email came from an approved source. This directly addresses the problem of legitimate emails being flagged.
Why the other options are incorrect:
A). Disable DKIM to avoid signature conflicts.This is incorrect because DKIM helps validate message authenticity by using digital signatures. Disabling it would weaken email validation rather than improve it.
B). Implement DMARC with a " reject " policy to enforce sender validation.DMARC is important, but a reject policy can cause legitimate messages to fail if SPF and DKIM are not configured correctly first. DMARC builds on SPF and DKIM; it does not replace the need to authorize all sending sources.
C). Replace the domain ' s MX record with the marketing provider ' s services.MX records control where incoming email is received, not which systems are authorized to send email. This would not solve the validation issue for outbound messages.
From a Security+ perspective, this question focuses on email security controls and proper configuration of SPF, DKIM, and DMARC. The most direct fix for multiple legitimate senders is to ensure the SPF record includes every authorized provider.

NEW QUESTION: 102
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: (SHOW ANSWER)
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: 103
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: 104
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: (SHOW ANSWER)
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. Reference = 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: 105
Which of the following could potentially be introduced at the time of side loading?
A. User impersonation
B. Rootkit
C. On-path attack
D. Buffer overflow
Answer: (SHOW ANSWER)
Side loading is the process of installing applications from unofficial sources, often bypassing standard app stores. This increases the risk of installing malicious software, such as a rootkit, which is a type of malware designed to provide persistent privileged access while hiding its presence.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Side loading applications from unofficial sources can introduce malware, such as rootkits, to the system." Exam Objectives 2.1: "Compare and contrast different types of threats."

NEW QUESTION: 106
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: (SHOW ANSWER)
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.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
According to various privacy rules and regulations, users have the power to request that all data pertaining to them is deleted. This is known as:

A. Right to be forgotten
B. Attestation and acknowledgement
C. Data retention
D. Information deletion
Answer: A (LEAVE A REPLY)
The right to be forgotten refers to an individual's legal right, under regulations such as GDPR, to request the deletion of all personal data held about them by an organization. This gives individuals control over their digital footprint and privacy.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "The right to be forgotten is a privacy right allowing individuals to request deletion of their personal data." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

NEW QUESTION: 108
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)
The correct answer is A. ICS.
ICS stands for Industrial Control Systems. These systems are commonly used in industrial environments such as manufacturing, energy, utilities, water treatment, transportation, and critical infrastructure. ICS environments often use proprietary protocols, specialized hardware, and legacy systems. They are designed to operate reliably for many years, sometimes in harsh physical environments, and may have limited remote management capabilities.
This aligns with CompTIA Security+ SY0-701 topics involving specialized systems, operational technology, embedded systems, and industrial control system security.
Why the other options are incorrect:
B). Microservers
Microservers are small, low-power servers used for lightweight workloads. They are not specifically associated with proprietary industrial controls or harsh operating environments.
C). Containers
Containers are lightweight application environments used to package and run software. They are not designed specifically for long-term industrial control in harsh environments.
D). IoT
Internet of Things devices can be embedded and may operate in many environments, but the description of proprietary controls, harsh environments, long operational lifespans, and limited remote management best matches ICS.
Therefore, the correct answer is ICS.

NEW QUESTION: 109
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: (SHOW ANSWER)
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: 110
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. Directory traversal
D. Privilege escalation
Answer: (SHOW ANSWER)

NEW QUESTION: 111
A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 002.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-BR	user1
10.18.04.38	EB-AC-11-02-42-F3	BC-CA	user3
10.18.04.59	20-BB-5A-11-52-3A	PC-PA	user2
10.18.04.58	20-BB-5A-D1-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-02-42-F3	WIN10	user3
10.18.04.2[illegible]	[illegible]	PC-NJ	admin

CompTIA
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. DNS hijacking let an attacker intercept the captive portal traffic.
D. An administrator bypassed the security controls for testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

A. Whaling
B. Credential harvesting
C. Prepending
D. Dumpster diving
Answer: (SHOW ANSWER)
Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security measures in cyber hygiene practices.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

NEW QUESTION: 113
Which of the following strategies most effectively protects sensitive data at rest in a database?
A. Hashing
B. Masking
C. Tokenization
D. Obfuscation
Answer: (SHOW ANSWER)
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: 114
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: 115
A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?
A. Concurrent session usage
B. Secure DNS cryptographic downgrade
C. On-path resource consumption
D. Reflected denial of service
Answer: (SHOW ANSWER)
A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

NEW QUESTION: 116
After multiple phishing simulations, 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: (SHOW ANSWER)
The correct answer is D. Gamification.Gamification uses game-like elements, rewards, points, competitions, badges, leaderboards, or incentives to encourage positive security behavior. In this scenario, employees are being incentivized not to click phishing links, which is a security awareness technique based on motivation and participation.Why the other options are incorrect: Computer-based trainingComputer-based training is a structured online training method. The question focuses on incentives, not simply online instruction.
Insider threat awarenessInsider threat awareness trains employees to recognize and report insider risks. The scenario is about phishing behavior and incentive-based awareness.SOAR playbookA SOAR playbook automates or standardizes security response actions.

NEW QUESTION: 117

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: (SHOW ANSWER)

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.

Reference = 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: 118

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: (SHOW ANSWER)

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.

NEW QUESTION: 119
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: (SHOW ANSWER)
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: 120
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?
Freecram.net
A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA
Answer: (SHOW ANSWER)
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
Reference:
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: 121
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: C (LEAVE A REPLY)
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.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?
A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software
Answer: (SHOW ANSWER)
A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

NEW QUESTION: 123
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116; Local Admin Accounts - Security Risks and Best Practices (Part 1)

NEW QUESTION: 124
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 following best describes 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. Reference = Insider Threats - CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

NEW QUESTION: 125
A security team identifies a vulnerability in an application that the developers will not be able to patch for six months. Which of the following should the security team use to document this vulnerability?
A. Risk register
B. Patching schedule
C. Vulnerability matrix
D. Change management procedure
Answer: (SHOW ANSWER)
The vulnerability should be documented in the risk register because it represents an identified risk that cannot be immediately remediated. A risk register tracks risk details such as description, owner, likelihood, impact, severity, mitigation strategy, acceptance status, review dates, and residual risk. Since the developers cannot patch the issue for six months, the organization needs formal visibility and accountability until remediation is possible. A patching schedule may track when updates are planned, but it does not fully document risk ownership and business impact. A vulnerability matrix may help prioritize technical findings, but it is not the central governance record. Change management procedures control changes, not long-term risk tracking.

NEW QUESTION: 126
An end-of-service server cannot be patched, but it still performs as expected for business operations. The team moves the system to a segmented network. Which of the following control types has the team applied?
A. Preventive
B. Deterrent
C. Corrective
D. Compensating
Answer: D (LEAVE A REPLY)

This is a compensating control because the organization cannot apply the preferred control, which would be patching or replacing the end-of-service server. Instead, it uses network segmentation to reduce exposure and limit the risk. A compensating control is an alternative safeguard used when the primary security requirement cannot be implemented due to technical, operational, or business constraints. Moving the server to a segmented network does not fix the vulnerability itself, so it is not corrective. It may reduce attack paths, but the key issue is that it substitutes for the missing patching capability. A deterrent control discourages unwanted behavior, such as warning signs or legal notices. A preventive control directly blocks incidents, but here the more precise classification is compensating.

NEW QUESTION: 127
A company experiences a data loss event due to a stolen laptop. In order to prevent future similar events, a security analyst must implement a scalable solution to ensure all data on company laptops remains secure in the event of theft or loss. Which of the following should the analyst do next?
A. Configure the HSM for each device and store recovery keys centrally.
B. Implement LAPS to ensure secure password rotation for administrative accounts.
C. Use an MDM platform to manage the devices and force security configurations.
D. Ensure that each laptop has the secure enclave properly initialized in the BIOS.
Answer: (SHOW ANSWER)
The best answer is C. Use an MDM platform to manage the devices and force security configurations.
The question asks for a scalable solution to protect data on company laptops if they are stolen or lost. An MDM (Mobile Device Management) platform is the best choice because it allows centralized administration of many endpoints and can enforce security controls across all laptops, such as:
full-disk encryption requirements
screen lock policies
remote wipe capabilities
compliance checks
device configuration enforcement
This makes MDM the most scalable and manageable approach for protecting a fleet of laptops.
Why the other options are incorrect:
A). Configure the HSM for each device and store recovery keys centrally.This is not the most practical or scalable answer for standard laptops, and HSMs are not typically configured individually this way for endpoint theft prevention.
B). Implement LAPS to ensure secure password rotation for administrative accounts.LAPS helps secure local administrator passwords, but it does not directly protect data at rest on a stolen laptop.
D). Ensure that each laptop has the secure enclave properly initialized in the BIOS.Hardware-based protections can help, but this is not the best broad, centrally managed, scalable control compared with MDM-enforced policies.
From a Security+ perspective, the main protection against data loss from stolen laptops is usually centralized device management with enforced encryption and security controls, making C the best answer.

NEW QUESTION: 128
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.

NEW QUESTION: 129
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: (SHOW ANSWER)
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. Reference = 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: 130
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: (SHOW ANSWER)
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: 131
Which of the following is used to add extra complexity before using a one-way data transformation algorithm?
A. Key stretching
B. Data masking
C. Steganography
D. Salting
Answer: (SHOW ANSWER)
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks. Reference = Passwords technical overview Encryption, hashing, salting - what's the difference?
Salt (cryptography)

NEW QUESTION: 132
An organization experiences a compromise in a cloud-hosted solution that contains customer information. Which of the following strategies will help determine the sensitivity level of the breach?
A. Permission restrictions
B. Tabletop exercise
C. Data classification
D. Asset inventory
Answer: (SHOW ANSWER)
The correct answer is Data classification because it is the primary mechanism used to determine the sensitivity and criticality of information involved in a security incident. According to the Security+ SY0-701 governance and risk management concepts, data classification assigns labels-such as public, internal, confidential, or restricted-to information based on its sensitivity, value to the organization, and potential impact if disclosed, altered, or destroyed. When a breach occurs, these classifications allow security teams and management to quickly assess how severe the incident is and what regulatory, legal, or business consequences may apply.
In this scenario, the compromised cloud-hosted solution contains customer information. By referencing the organization's data classification scheme, incident responders can determine whether the exposed data includes personally identifiable information (PII), financial data, health records, or other regulated data types. This directly influences breach notification requirements, incident escalation, response prioritization, and communication with stakeholders. The SY0-701 study guide emphasizes that effective security governance depends on having clearly defined classification standards before an incident occurs, so decisions during response are consistent and defensible.
The other options do not meet the goal of determining sensitivity. Permission restrictions are access control mechanisms used to prevent unauthorized access, not to evaluate the importance of data after a compromise. Tabletop exercises are preparedness and training activities designed to test incident response plans, not to classify real data. Asset inventory identifies systems, hardware, software, and data locations, but it does not define how sensitive the data is; it only helps locate what may be affected.
Therefore, data classification is the most appropriate strategy for determining the sensitivity level of the breach, aligning directly with Security+ SY0-701 objectives related to risk management, privacy, and incident impact assessment.

NEW QUESTION: 133

Which of the following metrics are used to calculate the risk rating in a matrix format? Select two.

A. Likelihood

B. Quantitative

C. SLE

D. Impact

E. ALE

F. ARO

Answer: (SHOW ANSWER)

The correct answers are A. Likelihood and D. Impact.

A risk matrix commonly calculates or represents risk using likelihood and impact. Likelihood measures the probability that a threat or risk event will occur. Impact measures the severity of the consequences if the event occurs. Together, they help determine the overall risk rating, such as low, medium, high, or critical.

For example:

Risk = Likelihood × Impact

Why the other options are incorrect:

B . Quantitative

Quantitative describes a type of risk analysis that uses numerical or monetary values. It is not one of the two standard matrix factors.

C . SLE

Single Loss Expectancy is used in quantitative risk calculations. It estimates the cost of a single incident.

E . ALE

Annualized Loss Expectancy is used in quantitative risk analysis and is commonly calculated as SLE × ARO.

F . ARO

Annualized Rate of Occurrence estimates how often an event is expected to happen per year. It is also used in quantitative risk calculations.

Therefore, the two metrics used in a risk matrix are likelihood and impact.

NEW QUESTION: 134

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

A. Key stretching

B. Tokenization

C. Data masking

D. Salting

Answer: (SHOW ANSWER)

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

NEW QUESTION: 135

A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Select two).

A. Directive

B. Deterrent
C. Corrective
D. Preventive
E. Technical
F. Detective
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following is a risk of conducting a vulnerability assessment?
A. A disruption of business operations
B. Reports of false positives
C. Unauthorized access to the system
D. Finding security gaps in the system
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 137
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. Internal auditing
B. Vulnerability scans
C. Third-party attestation
D. Penetration testing
Answer: (SHOW ANSWER)

NEW QUESTION: 138
During a penetration test, a vendor attempts to enter an unauthorized area using an access badge Which of the following types of tests does this represent?
A. Defensive
B. Passive
C. Offensive
D. Physical
Answer: (SHOW ANSWER)
Attempting to enter an unauthorized area using an access badge during a penetration test is an example of a physical test. This type of test evaluates the effectiveness of physical security controls, such as access badges, security guards, and locks, in preventing unauthorized access to restricted areas.

* Defensive and offensive testing typically refer to digital or network-based penetration testing strategies.
* Passive testing involves observing or monitoring but not interacting with the environment.

NEW QUESTION: 139
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 anddisplay 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. Reference: 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: 140
Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?
Freecram.net
A. Encryption
B. Hashing
C. Masking
D. Tokenization
Answer: (SHOW ANSWER)
Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

NEW QUESTION: 141
An unexpected and out-of-character email message from a Chief Executive Officer's corporate account asked an employee to provide financial information and to change the recipient's contact number. Which of the following attack vectors is most likely being used?
A. Business email compromise
B. Phishing

C. Brand impersonation
D. Pretexting
Answer: A (LEAVE A REPLY)
Business Email Compromise (BEC)is atargeted phishing attackin whichattackers impersonate executives or high-ranking officials(such as a CEO) to manipulate employees intotransferring money or providing sensitive data. Since the request is coming from the CEO's corporate email (possibly spoofed or compromised), this is aclassic example of BEC.
Phishing (B)is a broader term but typically involvesmassfraudulent emails rather than targeted executive impersonation.
Brand impersonation (C)involves faking a company's identity (e.g., fake PayPal emails).
Pretexting (D)involves social engineering tactics but does not necessarily involve email compromise.

NEW QUESTION: 142
Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?
A. Non-repudiation
B. Confidentiality
C. Integrity
D. Availability
Answer: (SHOW ANSWER)

NEW QUESTION: 143
An organization is developing a security program that conveys the responsibilities associated with the general operation of systems and software within the organization. Which of the following documents would most likely communicate these expectations?
A. Business continuity plan
B. Change management procedure
C. Acceptable use policy
D. Software development life cycle policy
Answer: (SHOW ANSWER)
Detailed
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: 144
Which of the following best explains a concern with OS-based vulnerabilities?
A. An exploit will 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)
The best answer is A. An exploit will give an attacker access to system functions that span multiple applications.
Operating system vulnerabilities are especially concerning because the OS sits underneath and supports many applications and services. If an attacker exploits an OS-level flaw, the impact can extend across the entire system and affect multiple applications, services, and security controls.

This makes OS-based vulnerabilities particularly serious because compromise at the operating system level can provide broad control over:
system processes
memory and storage access
user accounts and privileges
network services
multiple installed applications
Why the other options are incorrect:
B . The OS vendor's patch cycle is not frequent enough to mitigate the large number of threats.This is not a universal or defining concern with OS-based vulnerabilities.
C . Most users trust the core operating system features and may not notice if the system has been compromised.This may be true in some situations, but it is not the best explanation of the inherent risk of OS vulnerabilities.
D . Exploitation of an operating system vulnerability is typically easier than any other vulnerability.This is too absolute and not generally true.
From a Security+ standpoint, OS vulnerabilities are especially dangerous because they can affect the foundational functions of the system and potentially impact many applications at once, making A the best answer.

NEW QUESTION: 145
A security analyst learns that an attack vector, used as part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of the initial exploit. Which of the following logs should the analyst review first?
A. Endpoint
B. Application
C. Firewall
D. NAC
Answer: (SHOW ANSWER)
Detailed Firewall logs provide details of all network traffic, including connections to and from IoT devices. They are typically the first source of evidence for identifying the time of an exploit. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

NEW QUESTION: 146
Which of the following is most likely to be used as a just-in-time reference document within a security operations center?
A. Change management policy
B. Risk profile
C. Playbook
D. SIEM profile
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
A playbook is a step-by-step, just-in-time reference used by Security Operations Center (SOC) analysts when responding to security alerts, incidents, and suspicious activities. Playbooks provide documented procedures for common scenarios such as malware detection, phishing investigations, ransomware response, and account compromise.
According to the CompTIA Security+ SY0-701 exam framework, playbooks support incident response by reducing analyst guesswork and ensuring consistency. They include details such as triage steps, required tools, escalation paths, log sources, and containment actions. This makes playbooks the most suitable document for immediate reference during live investigations.

Change management policies (A) govern system or configuration changes, not SOC operations. Risk profiles (B) provide organizational risk overviews, not incident-response steps. SIEM profiles (D) define correlation rules or dashboards but are not procedural guides.
Therefore, the correct answer is playbooks, which enable efficient, standardized, and repeatable responses to operational security events.

NEW QUESTION: 147
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. Public key infrastructure
B. Key escrow
C. Public key encryption
D. Open public ledger
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?
A. Hacktivists
B. Script kiddies
C. Competitors
D. Shadow IT
Answer: (SHOW ANSWER)
Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit IT department approval. This is the most likely cause of introducing vulnerabilities on a corporate network by deploying unapproved software, as such software may not have been vetted for security compliance, increasing the risk of vulnerabilities.
Reference =
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: 149
Which of the following should an organization focus on the most when making decisions about vulnerability prioritization?
A. Exposure factor
B. CVSS
C. CVE
D. Industry impact
Answer: (SHOW ANSWER)
Detailed The Common Vulnerability Scoring System (CVSS) is a standardized metric used to assess the severity of vulnerabilities, aiding organizations in prioritizing their response based on risk. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Vulnerabilities, Section: "Vulnerability Prioritization and Metrics".

NEW QUESTION: 150

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

Freecram.net

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

NEW QUESTION: 151
An administrator investigating an incident is concerned about the downtime of a critical server due to a failed drive. Which of the following would the administrator use to estimate the time needed to fix the issue?
A. MTTR
B. MTBF
C. RTO
D. RPO
Answer: (SHOW ANSWER)
Mean Time To Repair (MTTR) is a key metric used to estimate the average time required to repair a failed component or system and restore it to operational status. In this case, the administrator would rely on MTTR to estimate how long it will take to fix the critical server's failed drive and get it back online.
Mean Time Between Failures (MTBF) measures the expected operational lifespan between failures, so it does not provide an estimate of repair time.
Recovery Time Objective (RTO) refers to the maximum allowable downtime for a system or service before unacceptable impact occurs, which is a planning metric rather than an actual repair time measure.
Recovery Point Objective (RPO) defines the maximum acceptable data loss measured in time and relates to backup frequency rather than repair duration.

Therefore, MTTR is the appropriate metric to estimate the time to fix a failed drive. This concept is detailed in the Resilience and Physical Security chapter within the Security Operations domain of the SY0-701 exam [6:Chapter 9 CompTIA Security+ Study Guide]

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
Which of the following security control types does an acceptable use policy best represent?
A. Detective
B. Compensating
C. Corrective
D. Preventive
Answer: (SHOW ANSWER)
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.
Reference = 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: 153
An employee used a company's billing system to issue fraudulent checks. The administrator is looking for evidence of other occurrences of this activity. Which of the following should the administrator examine?

A. Firewall logs
B. Application logs
C. Vulnerability scanner logs
D. IDS/IPS logs
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following is the best reason to complete an audit in a banking environment?
A. Regulatory requirement
B. Organizational change
C. Self-assessment requirement
D. Service-level requirement
Answer: (SHOW ANSWER)
A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.
Reference:
Official CompTIA Security+ Study Guide (SY0-701), page 507
Security+ (Plus) Certification | CompTIA IT Certifications 2

NEW QUESTION: 155
During a security incident, the security operations team identified sustained network traffic from a malicious IP address:
10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?
A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32
Answer: (SHOW ANSWER)
A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

Reference = Firewall Rules - CompTIA Security+ SY0-401: 1.2, Firewalls - SY0-601 CompTIA Security+ : 3.3, Firewalls - CompTIA Security+ SY0-501, Understanding Firewall Rules - CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall - CompTIA A+ 220-1102 - 1.6.

NEW QUESTION: 156
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: (SHOW ANSWER)
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: 157
Which of the following is die most important security concern when using legacy systems to provide production service?
A. Instability
B. Lack of vendor support
C. Loss of availability
D. Use of insecure protocols
Answer: (SHOW ANSWER)
The most important security concern when using legacy systems is the lack of vendor support. Without support from the vendor, systems may not receive critical security patches and updates, leaving them vulnerable to exploitation. This lack of support can result in increased risk of security breaches, as vulnerabilities discovered in the software may never be addressed.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the context of risk management and the challenges posed by legacy systems.

NEW QUESTION: 158
Which of the following must be considered when designing a high-availability network? (Choose two).
A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication
Answer: A,E (LEAVE A REPLY)
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:
Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.
The other options are not directly related to high-availability network design:
Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.
Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

NEW QUESTION: 159
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: 160

A security technician determines that no additional patches can be applied to an application and the risks of operating as such must be accepted. Additionally, only a limited number of network services should utilize the application. Which of the following best describes this type of mitigation?

Freecram.net

A. Patching
B. Segmentation
C. Isolation
D. Monitoring
Answer: (SHOW ANSWER)
The best answer is C. Isolation.
The question describes an application that can no longer be patched, meaning the organization must continue operating it while accepting some risk. To reduce exposure, the application should only be used by a limited number of network services. This points to isolation, which means restricting the application's interaction with the rest of the environment to contain risk.
Isolation is commonly used for:
legacy systems
unsupported applications
unpatchable systems
high-risk services that must remain operational
By isolating the application, the organization limits the paths through which it can be attacked and reduces the chance that a compromise will spread to other systems.
Why the other options are incorrect:
A). PatchingThe question clearly states that no additional patches can be applied.
B). SegmentationSegmentation is related and often used as a method to isolate systems, but the question asks for the best description of the mitigation approach overall. Since the application is being restricted because it is risky and unpatchable, isolation is the stronger answer.
D). MonitoringMonitoring helps detect issues but does not directly reduce exposure in the way described.
From the SY0-701 perspective, when a vulnerable or unsupported application must remain in use, the preferred mitigation is often to isolate it from the broader environment. Therefore, C is the best answer.

NEW QUESTION: 161

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: 162

Which of the following actions best addresses a vulnerability found on a company's web server?

A. Patching

B. Segmentation

C. Monitoring

D. Decommissioning

Answer: (SHOW ANSWER)

NEW QUESTION: 163

Which of the following methods will most likely be used to identify legacy systems?

A. Bug bounty program

B. Vulnerability scan

C. Package monitoring

D. Dynamic analysis

Answer: (SHOW ANSWER)

A vulnerability scan is the most effective method for identifying legacy systems within an environment. Vulnerability scanners assess hosts for outdated operating systems, unsupported software versions, missing patches, deprecated services, and known Common Vulnerabilities and Exposures (CVEs). CompTIA Security+ SY0-701 highlights vulnerability scanning as a foundational security operation used to gain visibility into system age, patch status, and configuration weaknesses.

Legacy systems often stand out in scan results because they run end-of-life operating systems, use deprecated protocols, or lack current security updates. These indicators allow security teams to quickly flag systems that require isolation, compensating controls, or replacement.

Bug bounty programs (A) rely on external researchers and are not designed to inventory internal assets. Package monitoring (C) tracks software behavior and changes but does not identify system age or support status. Dynamic analysis (D) evaluates running applications for vulnerabilities, not infrastructure lifecycle status.

Because vulnerability scans provide broad visibility into system versions and supportability, the correct answer is B: Vulnerability scan.

NEW QUESTION: 164

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

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

NEW QUESTION: 165
An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).
A. Document default passwords.
B. Disable default accounts.
C. Remove unnecessary services.
D. Add the server to the asset inventory.
E. Send server logs to the SIEM.
F. Join the server to the corporate domain.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
A systems administrator is redesigning now devices will perform network authentication. The following requirements need to be met:
* An existing Internal certificate must be used.
* Wired and wireless networks must be supported
* Any unapproved device should be Isolated in a quarantine subnet
* Approved devices should be updated before accessing resources
Which of the following would best meet the requirements?
A. 802.IX
B. EAP
C. RADIUS
D. WPA2
Answer: (SHOW ANSWER)
802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167

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: (SHOW ANSWER)
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: 168
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?
A. SCAP
B. Net Flow
C. Antivirus
D. DLP
Answer: (SHOW ANSWER)
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

NEW QUESTION: 169
Which of the following provides the details about the terms of a test with a third-party penetration tester?
A. Rules of engagement
B. Supply chain analysis
C. Right to audit clause
D. Due diligence
Answer: (SHOW ANSWER)
Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:
The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
The testing team credentials and the authorized tools and techniques that they can use.
The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.

The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
The timeline and duration of the test, and the hours of operation and testing windows.
The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.
Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.
Reference = https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/
https://bing.com/search?q=rules+of+engagement+penetration+testing

NEW QUESTION: 170

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?

Freecram.net

A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response
Answer: (SHOW ANSWER)
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: 171
The management team notices that new accounts that are set up manually do not always have correct access or permissions.
Which of the following automation techniques should a systems administrator use to streamline account creation?
A. Guard rail script
B. Ticketing workflow
C. Escalation script
D. User provisioning script
Answer: (SHOW ANSWER)
A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources12.
The other options are not automation techniques that can streamline account creation:
Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software3.
Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process4.

Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage. Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

NEW QUESTION: 172
An organization experiences a suspected data breach that affects sensitive client information. The incident response team must preserve logs, server images, and email communications related to the breach. Which of the following best describes this course of action?
A. Maintaining the chain of custody
B. Performing root cause analysis
C. Enforcing a legal hold
D. Conducting a containment activity
Answer: (SHOW ANSWER)
A legal hold is the correct answer because the organization is preserving potentially relevant evidence after a suspected breach involving sensitive client information. In incident response and governance, legal hold prevents deletion, alteration, or routine retention-policy destruction of data that may be required for litigation, regulatory investigation, discovery, or internal investigation. Logs, server images, and email communications are exactly the kinds of records that may become evidence. Chain of custody is related but narrower: it documents who handled evidence, when, and how integrity was maintained. Root cause analysis happens later to determine why the breach occurred. Containment focuses on stopping spread or limiting damage. Here, the key action is preservation of records.

NEW QUESTION: 173
During a routine audit, an analyst discovers that a department at a high school uses a simulation program that was not properly vetted before deployment. Which of the following threats is this an example of?
A. Espionage
B. Data exfiltration
C. Shadow IT
D. Zero-day
Answer: (SHOW ANSWER)
The correct answer is C. Shadow IT.Shadow IT refers to hardware, software, cloud services, or applications used within an organization without formal approval, review, or oversight by the IT or security department. In this scenario, the department deployed a simulation program without proper vetting, making it an example of shadow IT.This aligns with CompTIA Security+ SY0-701 risk management and governance concepts. Unauthorized or unapproved technology can introduce risks such as data leakage, insecure configurations, licensing violations, compliance issues, privacy concerns, and unsupported software vulnerabilities.Why the other options are incorrect:
Answe r: EspionageEspionage involves spying or gathering confidential information for political, competitive, or financial advantage. The question does not indicate spying.
Answe r: Data exfiltrationData exfiltration is the unauthorized transfer of data out of an organization. The question only states that unvetted software was deployed.
Answe r: Zero-dayA zero-day is a vulnerability that is unknown to the vendor or has no available patch. The question does not describe an unknown vulnerability.Therefore, the best answer is shadow IT.

NEW QUESTION: 174
A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 002.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-BA	user1
10.18.04.38	EB-AC-11-02-42-F3	BC-CA	user3
10.18.04.59	28-BB-5A-11-52-3A	PC-PA	user2
10.18.04.58	28-BB-5A-D1-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-02-42-F3	WIN10	user3
10.18.04.2[illegible]	[illegible]	PC-NJ	admin

CompTIA
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.
Reference =
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: 175
Which of the following is an example of a data protection strategy that uses tokenization?
A. Encrypting databases containing sensitive data
B. Replacing sensitive data with surrogate values
C. Removing sensitive data from production systems
D. Hashing sensitive data in critical systems
Answer: (SHOW ANSWER)
Detailed
Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Masking and Tokenization".

NEW QUESTION: 176
Which of the following is a reason environmental variables are a concern when reviewing potential system vulnerabilities?
A. The contents of environmental variables could affect the scope and impact of an exploited vulnerability.
B. In-memory environmental variable values can be overwritten and used by attackers to insert malicious code.
C. Environmental variables define cryptographic standards for the system and could create vulnerabilities if deprecated algorithms are used.
D. Environmental variables will determine when updates are run and could mitigate the likelihood of vulnerability exploitation.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 177
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 internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password

CompTIA
freecram.net

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

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

freecramm.net

NEW QUESTION: 178
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: (SHOW ANSWER)
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: 179
A user needs to complete training at https://comptiatraining.com. After manually entering the URL, the user sees that the accessed website is noticeably different from the standard company website. Which of the following is the most likely explanation for the difference?
A. Cross-site scripting
B. Pretexting
C. Typosquatting
D. Vishing
Answer: (SHOW ANSWER)
Typosquatting(also known asURL hijacking) is a type of attack where cybercriminals register domain names similar to legitimate sites but with slight misspellings (e.g., comptiatraning.com instead of comptiatraining.com). Attackers use these fake sites tosteal credentials or distribute malware. Since the user manually entered the URL and reached an unexpected website,this strongly indicates a typosquatting attack.

NEW QUESTION: 180
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?
Freecram.net
A. Wireless access point
B. Switch
C. Firewall
D. NAC
Answer: (SHOW ANSWER)

Many IoT devices connect to the network via wireless access points. Reviewing these logs would reveal when the IoT device first connected, as well as any suspicious or anomalous traffic patterns associated with the exploit's initiation.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.1: "Wireless access point logs can help determine initial connectivity and exploitation of IoT devices." Exam Objectives 4.1: "Summarize the importance of logging and monitoring activities."

NEW QUESTION: 181
A systems administrator discovers a system that is no longer receiving support from the vendor. However, this system and its environment are critical to running the business, cannot be modified, and must stay online. Which of the following risk treatments is the most appropriate in this situation?
A. Refect
B. Transfer
C. Accept
D. Avoid
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182
A government official receives a blank envelope containing photos and a note instructing the official to wire a large sum of money by midnight to prevent the photos from being leaked on the Internet. Which of the following best describes the threat actor's intent?
A. Organized crime
B. Philosophical beliefs
C. Espionage
D. Blackmail
Answer: (SHOW ANSWER)
The threat actor's intent is clearly blackmail, a form of extortion where sensitive information is used to coerce an individual into taking an action, usually involving financial gain. In this scenario, the attacker threatens to leak incriminating or compromising photos unless the government official wires a large sum of money. CompTIA Security+ SY0-701 defines blackmail as the use of sensitive or embarrassing information to manipulate or force actions from victims.
This differs from organized crime (A), which focuses on profit-driven cyber operations but typically uses technical attacks such as ransomware, data theft, or fraud rather than anonymous mailed threats. Philosophical beliefs (B) refers to hacktivism, where attackers pursue ideological motives-not present here. Espionage (C) involves intelligence gathering for political or competitive advantage, typically performed by nation-states or advanced persistent threats (APTs).
This scenario aligns directly with extortion-based social engineering, where attackers manipulate victims through fear and emotional pressure. According to Security+ guidance, blackmail often occurs through email, physical mail, or compromised personal data leaks, all fitting this situation. Therefore, the threat actor's intent is blackmail.

NEW QUESTION: 183
Which of the following explains how organizations benefit from SCAP?
A. The configurations defined as part of established baselines allow organizations to deploy well-tested security solutions quickly and easily.
B. The consolidated reporting layout makes it easier for technicians to communicate incident response to senior decision-makers.
C. The common format for vulnerability scanning and reporting enables greater interoperability between security tools from different vendors.
D. The strict compliance to international standards reduces overall cost and risk to organizations when a security breach occurs.
Answer: (SHOW ANSWER)
The best answer is C. The common format for vulnerability scanning and reporting enables greater interoperability between security tools from different vendors.
SCAP (Security Content Automation Protocol) is a standardized framework that helps security tools use common methods for expressing, measuring, and reporting security issues such as vulnerabilities, misconfigurations, and compliance results. One of its biggest benefits is interoperability across tools from different vendors.
Because SCAP uses standardized formats and naming conventions, organizations can more easily:
share scan results
compare findings across platforms
automate vulnerability and compliance checks
integrate multiple security products
Why the other options are incorrect:
A). The configurations defined as part of established baselines allow organizations to deploy well-tested security solutions quickly and easily.Baselines are important, but this answer is too general and does not capture the main benefit of SCAP.
B). The consolidated reporting layout makes it easier for technicians to communicate incident response to senior decision-makers.SCAP is not primarily about incident response reporting to executives.
D). The strict compliance to international standards reduces overall cost and risk to organizations when a security breach occurs.This is too broad and not the clearest explanation of what SCAP actually provides.
From the SY0-701 perspective, SCAP is valuable because it supports standardized vulnerability and configuration assessment and improves tool interoperability. Therefore, C is the correct answer.

NEW QUESTION: 184
The Cyber Incident Response Team is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The team found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?
A. WAF utilizing SSL decryption
B. NGFW utilizing application inspection
C. UTM utilizing a threat feed
D. SD-WAN utilizing IPsec
Answer: (SHOW ANSWER)
The correct answer is B. NGFW utilizing application inspection.
A next-generation firewall, or NGFW, can perform deep packet inspection and application-layer inspection. This allows it to identify the actual application or protocol being used, even when the traffic is running over a nonstandard port.
In this scenario, HTTP traffic is being sent over port 53. Port 53 is normally associated with DNS, so a traditional port-based firewall might allow or misclassify the traffic. An NGFW with application inspection could detect that the traffic is actually HTTP, not DNS, and block it according to policy.

Why the other options are incorrect:
A . WAF utilizing SSL decryption
A web application firewall protects web applications from web-based attacks. SSL decryption helps inspect encrypted HTTPS traffic, but this scenario is about detecting HTTP over an unusual port.
C . UTM utilizing a threat feed
A Unified Threat Management device can provide multiple security functions, and threat feeds can help identify known malicious indicators. However, the key control needed here is application inspection.
D . SD-WAN utilizing IPsec
SD-WAN manages WAN connectivity and routing, while IPsec provides encrypted tunnels. This does not identify or block HTTP being misused over port 53.
Therefore, the best answer is NGFW utilizing application inspection.

NEW QUESTION: 185
Which of the following architecture models ensures that critical systems are physically isolated from the network to prevent access from users with remote access privileges?
A. Segmentation
B. Virtualized
C. Air-gapped
D. Serverless
Answer: (SHOW ANSWER)
Anair-gapped (C)system is completely isolated from unsecured networks (like the internet) and other systems, preventing any form of remote access. This is often used in highly sensitive environments such as military, nuclear, or critical infrastructure systems.
This is mentioned underDomain 3.4: Given a scenario, apply cybersecurity resilience conceptsin the CompTIA Security+ SY0-701 Exam Objectives, specifically under"Isolation (e.g., air-gapped)".

NEW QUESTION: 186
A systems administrator receives an alert that a company's internal file server is very slow and is only working intermittently. The systems administrator reviews the server management software and finds the following information about the server:

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

Which of the following indicators most likely triggered this alert?
A. Account lockout
B. Resource consumption
C. Concurrent session usage
D. Network saturation
Answer: (SHOW ANSWER)
NEW QUESTION: 187
Which of the following should be used to ensure that a new software release has not been modified before reaching the user?
A. Tokenization
B. Encryption
C. Hashing

D. Obfuscation

Answer: (SHOW ANSWER)

Hashing is the correct mechanism for ensuring that a software release has not been modified prior to reaching the end user. Hashing provides integrity verification by generating a fixed-length digest (such as SHA-256) from the original software package. When users download the software, they can compute the hash locally and compare it to the hash value published by the vendor. If the values match, the software has not been altered; if they differ, tampering or corruption has occurred.

CompTIA Security+ SY0-701 emphasizes hashing as a core cryptographic control used to verify integrity for files, updates, patches, and software distributions. Hashing is extremely sensitive to change-altering even a single bit in the file results in a completely different hash value.

Encryption (B) protects confidentiality, not integrity. Tokenization (A) replaces sensitive data with tokens and is unrelated to software integrity.

Obfuscation (D) makes code harder to read but does not guarantee it has not been modified.

Therefore, hashing is the most appropriate and reliable method to ensure software integrity before release.

NEW QUESTION: 188

A company performs risk analysis on its equipment and estimates it will experience about ten incidents over a five-year period. Which of the following is the correct ARO for the equipment?

A. 2

B. 5

C. 10

D. 50

Answer: (SHOW ANSWER)

The best answer is A. 2.

ARO (Annualized Rate of Occurrence) measures how many times an incident is expected to occur per year.

The company expects:

10 incidents

over 5 years

So the calculation is:

ARO = 10 / 5 = 2

This means the expected annual rate of occurrence is 2 incidents per year.

Why the other options are incorrect:

B). 5This would not represent the yearly average based on the numbers given.

C). 10This is the total number of incidents over five years, not the annualized value.

D). 50This is not supported by the information in the question.

From a Security+ risk calculation standpoint, when a total event count is spread across multiple years, the ARO is found by dividing the total incidents by the number of years. Therefore, A is correct.

NEW QUESTION: 189

A security company informs its customers of a new vulnerability that affects web applications. The vulnerability does not have an available patch at the moment. Which of the following best describes this vulnerability?

A. Zero-day

B. XSS

C. SQLi

D. Buffer overflow

Answer: (SHOW ANSWER)

The best answer is A. Zero-day.

A zero-day vulnerability is a newly discovered vulnerability for which no patch or official fix is yet available. Because defenders have had zero days to fully remediate it, attackers may be able to exploit it before a vendor releases a patch.

The question specifically states that the vulnerability is new and does not have an available patch, which is the defining clue.

Why the other options are incorrect:

B . XSSCross-site scripting is a specific web application attack type, not a description of whether a patch exists.

C . SQLiSQL injection is also a specific attack type, not the broader vulnerability status being asked about.

D . Buffer overflowBuffer overflow is a type of coding flaw, but again it does not specifically describe the condition of having no patch available.

From a Security+ perspective, when a vulnerability is newly identified and lacks a vendor fix, it is best described as a zero-day.

NEW QUESTION: 190

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

Freecram.net

A. Software development life cycle

B. Risk tolerance

C. Certificate signing request

D. Maintenance window

Answer: (SHOW ANSWER)

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: 191

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: (SHOW ANSWER)
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: 192
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: (SHOW ANSWER)
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: 193
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: 194
Which of the following allows for the attribution of messages to individuals?
A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs
Answer: (SHOW ANSWER)
Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document. Reference = Non-repudiation - CompTIA Security+ SY0-701 - 1.2, CompTIA Security+ SY0-301: 6.1 - Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

NEW QUESTION: 195
The private key for a website was stolen, and a new certificate has been issued. Which of the following needs to be updated next?
A. OCSP
B. CSR
C. SCEP
D. CRL
Answer: (SHOW ANSWER)

NEW QUESTION: 196
An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: D (LEAVE A REPLY)

Detailed
Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Controls for Financial Systems".

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 197
Which of the following should an organization use to protect its environment from external attacks conducted by an unauthorized hacker?
A. IDS
B. HIDS
C. NIPS
D. ACL
Answer: (SHOW ANSWER)

NEW QUESTION: 198
A new employee can select a particular make and model of an employee workstation from a preapproved list. Which of the following is this an example of?
A. MDM
B. CYOD
C. PED
D. COPE
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
The described scenario is CYOD (Choose Your Own Device). In a CYOD model, employees may choose from a list of company-approved devices. These devices are vetted for compatibility, security, and organizational standards while still providing some flexibility to employees.
The SY0-701 exam differentiates CYOD from other mobile deployment models:
COPE (D) - Company-Owned, Personally Enabled: devices are company-owned and fully managed, but employees can use them personally.
MDM (A) - Mobile Device Management: a tool, not a deployment model, used for managing configurations and security on devices.
PED (C) - Portable Electronic Device: a generic category, not a deployment strategy.
CYOD strikes a balance between employee preference and maintaining a secure, standardized environment. It reduces risk associated with BYOD while avoiding the rigidity of COPE. CYOD also supports consistent patching, support, and security enforcement because all devices meet the organization's baseline criteria.
This aligns with the Security Architecture section of SY0-701, where the exam stresses secure device deployment strategies and maintaining uniform controls over endpoint assets.

NEW QUESTION: 199

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: (SHOW ANSWER)

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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION: 200

A website user is locked out of an account after clicking an email link and visiting a different website Web server logs show the user's password was changed, even though the user did not change the password. Which of the following is the most likely cause?

Freecram.net

A. Cross-sue request forgery

B. Directory traversal

C. ARP poisoning

D. SQL injection

Answer: (SHOW ANSWER)

The scenario describes a situation where a user unknowingly triggers an unwanted action, such as changing their password, by clicking a malicious link. This is indicative of a Cross-Site Request Forgery (CSRF) attack, where an attacker tricks the user into executing actions they did not intend to perform on a web application in which they are authenticated.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common attack vectors like CSRF.

NEW QUESTION: 201

Which of the following can automate vulnerability management?

A. CVE

B. SCAP

C. OSINT

D. CVSS

Answer: (SHOW ANSWER)

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: 202
Which of the following best explains why an organization would choose a warm site for disaster recovery?
A. It reduces complexity by replicating data in real time across identical environments.
B. It eliminates the need for backup testing by using cloud-native infrastructure.
C. It offers fully automated fail over with no manual intervention required.
D. It balances cost and recovery time by maintaining partially configured systems.
Answer: (SHOW ANSWER)
A warm site is chosen because it provides a practical balance between cost and recovery speed. It is partially prepared with infrastructure, network connectivity, and sometimes replicated or recent backup data, but it usually still requires some configuration, restoration, or activation before full operations resume. A hot site is more expensive because it is fully operational or nearly real-time synchronized, which better matches option A or C. A cold site is cheaper but slower because it may only provide space, power, and basic facilities. Backup testing is still required regardless of the recovery model, so option B is incorrect. In Security+, warm sites sit between cold and hot sites for recovery time objective and cost.

NEW QUESTION: 203
Which of the following most securely protects data at rest?
A. TLS 1.2
B. AES-256
C. Masking
D. Salting
Answer: (SHOW ANSWER)
AES-256 is a symmetric encryption algorithm widely used to protect data at rest by converting plaintext into ciphertext that is unreadable without the proper key. It provides strong confidentiality and is a standard for encrypting stored data.
TLS 1.2 (A) secures data in transit, not at rest. Masking (C) obscures data but typically for display or limited use and is reversible. Salting (D) is used alongside hashing to protect passwords and data integrity but does not encrypt data.
Encryption with AES-256 is recognized as a best practice for securing stored data in the Security+ Cryptography and General Security Concepts domains#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 204
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: (SHOW ANSWER)
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. Reference = 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: 205
A security consultant is working with a client that wants to physically isolate its secure systems. Which of the following best describes this architecture?
A. Air gapped
B. Containerized
C. SDN
D. Highly available
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which of the following exercises should an organization use to improve its incident response process?
A. Tabletop
B. Replication
C. Failover
D. Recovery
Answer: (SHOW ANSWER)
A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

NEW QUESTION: 207
A vendor needs to remotely and securely transfer files from one server to another using the command line. Which of the following protocols should be Implemented to allow for this type of access? (Select two).
A. SSH
B. SNMP
C. RDP
D. S/MIME
E. SMTP
F. SFTP
Answer: (SHOW ANSWER)
Secure Shell (SSH) is a protocol used for secure command-line access to remote systems, while Secure File Transfer Protocol (SFTP) is an extension of SSH used specifically for securely transferring files. Both SSH and SFTP ensure that data is encrypted during transmission, protecting it from interception or tampering.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

NEW QUESTION: 208
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: 209
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: 210
After failing an audit twice, an organization has been ordered by a government regulatory agency to pay fines. Which of the following caused this action?
Freecram.net
A. Rules of engagement
B. Contract violations
C. Non-compliance
D. Government sanctions
Answer: (SHOW ANSWER)

NEW QUESTION: 211
An organization plans to increase security controls for devices that connect to its internal network. The additional security control must perform port-based authentication as part of the connection process. Which of the following should the organization implement?
A. EDR
B. SASE

C. 802.1X
D. WPA3
Answer: (SHOW ANSWER)
802.1X is the correct answer because it provides port-based network access control. It authenticates devices or users before allowing access through a switch port or wireless access point. In a typical deployment, the supplicant is the endpoint, the authenticator is the switch or access point, and the authentication server is often RADIUS. This allows an organization to prevent unauthorized devices from connecting to the internal network. EDR protects endpoints by detecting and responding to threats, but it does not provide port-based authentication. SASE is a cloud-delivered security architecture for secure access and networking. WPA3 strengthens wireless encryption and authentication, but the phrase "port-based authentication" specifically identifies 802.1X. Therefore, 802.1X best satisfies the requirement.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 212
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: (SHOW ANSWER)
Detailed 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: 213
Which of the following is the final step of the modem response process?
A. Lessons learned
B. Eradication
C. Containment
D. Recovery
Answer: (SHOW ANSWER)
The final step in the incident response process is "Lessons learned." This step involves reviewing and analyzing the incident to understand what happened, how it was handled, and what could be improved. The goal is to improve future response efforts and prevent similar incidents from occurring. It's essential for refining the incident response plan and enhancing overall security posture.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of incident response and recovery.

NEW QUESTION: 214

Which of the following Is a common, passive reconnaissance technique employed by penetration testers in the early phases of an engagement?
A. Exploit validation
B. Port scanning
C. Open-source intelligence
D. Pivoting
Answer: (SHOW ANSWER)

NEW QUESTION: 215
A security analyst is creating base for the server team to follow when hardening new devices for deployment. Which of the following beet describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide
Answer: D (LEAVE A REPLY)
The security analyst is creating a "secure configuration guide," which is a set of instructions or guidelines used to configure devices securely before deployment. This guide ensures that the devices are set up according to best practices to minimize vulnerabilities and protect against potential security threats.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on System Hardening and Secure Configuration.

NEW QUESTION: 216
A company processes personal data from customers in multiple countries. Which of the following actions is most critical for maintaining legal compliance with global privacy regulations?
A. Storing all customer data on encrypted local servers
B. Hiring a data privacy officer to review contracts
C. Ensuring DPAs are in place with third-party vendors
D. Using strong passwords and firewalls on all endpoints
Answer: (SHOW ANSWER)
The best answer is C. Ensuring DPAs are in place with third-party vendors.
When a company handles personal data across multiple countries, one of the most important legal and regulatory requirements is ensuring that any third parties processing that data are contractually bound to protect it appropriately. A DPA (Data Processing Agreement) defines how a vendor may collect, process, store, share, and protect personal data. This is a key requirement in many privacy frameworks and regulations.
This matters because organizations are often still responsible for customer data even when a third-party provider handles it. A DPA helps establish:
the roles and responsibilities of each party
the legal basis and limits for data processing
security and privacy obligations
breach notification expectations
cross-border data handling requirements
Why the other options are incorrect:

A). Storing all customer data on encrypted local serversEncryption is important, but this alone does not ensure compliance with international privacy laws. Legal compliance involves governance, lawful processing, third- party handling, and contractual obligations.
B). Hiring a data privacy officer to review contractsA privacy officer may be helpful or required in some situations, but simply hiring one is not as directly critical as having the actual data processing agreements in place.
D). Using strong passwords and firewalls on all endpointsThese are valuable security controls, but they are not sufficient for legal compliance with global privacy regulations.
From a Security+ perspective, privacy compliance often involves third-party risk management, contractual controls, and lawful data handling, making DPAs the most critical answer here.

NEW QUESTION: 217
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: (SHOW ANSWER)
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

NEW QUESTION: 218
Which of the following is used to validate a certificate when it is presented to a user?
A. OCSP
B. CSR
C. CA
D. CRC
Answer: (SHOW ANSWER)
OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

NEW QUESTION: 219
Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?
A. Deploy a SIEM solution
B. Create custom scripts to aggregate and analyze logs
C. Implement EDR technology
D. Install a unified threat management appliance
Answer: (SHOW ANSWER)

Deploying a Security Information and Event Management (SIEM) solution allows for efficient log aggregation, correlation, and analysis across an organization's infrastructure, providing real-time security insights.Reference: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

NEW QUESTION: 220

A security analyst receives an alert from a web server that contains the following logs:
GET /image?filename=../../../etc/passwd
Host: AcmeInc.web.net
useragent: python-request/2.27.1
GET /image?filename=../../../etc/shadow
Host: AcmeInc.web.net
useragent: python-request/2.27.1
Which of the following attacks is being attempted?

Freecram.net

A. File injection
B. Privilege escalation
C. Directory traversal
D. Cookie forgery
Answer: (SHOW ANSWER)
The log entries clearly show an attacker attempting to access sensitive system files by manipulating the filename parameter. The use of ../../../ is a classic indicator of a directory traversal attack, also called path traversal. This technique is used to move outside the intended web directory and access restricted locations on the server's filesystem.
In this case, the attacker is attempting to read:
/etc/passwd - contains user account information
/etc/shadow - contains hashed password entries and is even more sensitive The CompTIA Security+ SY0-701 exam describes directory traversal as an attack where unvalidated user input allows navigation to system directories, often using sequences like ../ to bypass file path restrictions. This is exactly what is shown in the logs.
File injection (A) would involve inserting malicious files or code, not reading system files.
Privilege escalation (B) requires exploiting a system to gain higher privileges, not just reading files.
Cookie forgery (D) involves manipulating session cookies and does not match the observed behavior.
Because the attacker is using path traversal patterns to access protected files, the correct answer is C. Directory traversal.

NEW QUESTION: 221
A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?
A. Visualization and isolation of resources
B. Network segmentation
C. Data encryption
D. Strong authentication policies
Answer: (SHOW ANSWER)
When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated environments (e.g., virtual machines or containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.
* Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.
* Data encryption is also essential but doesn't specifically address resource isolation in a cloud environment.

* Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

NEW QUESTION: 222
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: (SHOW ANSWER)
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: 223
Which of the following is the most relevant reason a DPO would develop a data inventory?
A. To automate the reduction of duplicated data
B. To extend the length of time data can be retained
C. To determine the impact in the event of a breach
D. To manage data storage requirements better
Answer: (SHOW ANSWER)

NEW QUESTION: 224
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: (SHOW ANSWER)
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: 225
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: (SHOW ANSWER)
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: 226
A penetration tester visits a client's website and downloads the site's content. Which of the following actions is the penetration tester performing?
A. Unknown environment testing
B. Vulnerability scan
C. Due diligence
D. Passive reconnaissance
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
The described activity-visiting a website and downloading publicly accessible content-is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.
According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:
Public websites
DNS records
News articles
Metadata
Public document repositories
The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic.
Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning. Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.
Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in

the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
Which of the following are the best security controls for controlling on-premises access? (Select two.)
A. Swipe card
B. Picture ID
C. Phone authentication application
D. Biometric scanner
E. Camera
F. Memorable
Answer: (SHOW ANSWER)
Detailed Swipe cards and biometric scanners are commonly used to control on-premises access due to their reliability and ability to restrict unauthorized entry. Swipe cards provide physical access control, while biometric scanners ensure identity verification. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 1: General Security Concepts, Section: "Physical Security Controls".

NEW QUESTION: 228
Which of the following is best prevented by adding input validation to an AI chatbot?
A. Model manipulation
B. Bias
C. Prompt injection
D. Hallucinations
Answer: (SHOW ANSWER)
Input validation is most directly used to reduce prompt injection attacks against AI chatbots. Prompt injection occurs when a user enters crafted instructions designed to override, bypass, or manipulate the chatbot's intended system instructions. By validating, filtering, constraining, and sanitizing user input, an organization can prevent malicious instructions from being interpreted as trusted commands. Model manipulation is broader and may include poisoning or adversarial techniques beyond simple input validation. Bias is mainly addressed through training data governance, testing, and model evaluation. Hallucinations are inaccurate or fabricated AI outputs, usually reduced through grounding, retrieval controls, and output verification. Therefore, for a chatbot, input validation best maps to preventing prompt injection.

NEW QUESTION: 229
A security manager is implementing MFA and patch management. Which of the following would best describe the control type and category? (Select two).
A. Physical
B. Managerial
C. Detective

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

NEW QUESTION: 230
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?
Freecram.net
A. Change management ticketing system
B. Behavioral analyzer
C. Collaboration platform
D. Version control tool
Answer: (SHOW ANSWER)
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: 231
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.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

NEW QUESTION: 232

An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve this objective?

A. Red teaming

B. Penetration testing

C. Independent audit

D. Vulnerability assessment

Answer: (SHOW ANSWER)

The correct answer is C. Independent audit.

An independent audit provides objective assurance that security controls are properly designed, implemented, and operating effectively. Audits are commonly used to validate compliance, governance, risk management, and control effectiveness.

This aligns with CompTIA Security+ SY0-701 topics involving audits, assessments, governance, compliance, and third-party assurance.

Why the other options are incorrect:

A . Red teaming

Red teaming simulates real-world adversary behavior to test detection and response capabilities. It does not provide the same formal assurance over control design and operating effectiveness.

B . Penetration testing

Penetration testing identifies exploitable vulnerabilities, but it does not comprehensively verify that all controls are properly designed and operating effectively.

D . Vulnerability assessment

A vulnerability assessment identifies and prioritizes weaknesses, but it does not provide formal assurance of control design and operating effectiveness.

Therefore, the best answer is independent audit.

NEW QUESTION: 233

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: (SHOW ANSWER)

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: 234

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

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

NEW QUESTION: 235
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. Shadow IT
B. Data exfiltration
C. Espionage
D. Nation-state attack
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which of the following provides the best protection against unwanted or insecure communications to and from a device?
A. System hardening
B. Host-based firewall
C. Intrusion detection system
D. Anti-malware software
Answer: (SHOW ANSWER)
A host-based firewall controls incoming and outgoing network traffic on a device by enforcing security rules, effectively blocking unwanted or insecure communications. It is specifically designed to protect the device from unauthorized access and malicious traffic.
System hardening (A) reduces vulnerabilities by disabling unnecessary services and patching but does not control communications dynamically. Intrusion detection systems (C) detect suspicious traffic but typically do not block it (unless paired with prevention). Anti-malware (D) protects against malicious software but not directly network communication filtering.
Host-based firewalls are a fundamental component of endpoint security highlighted in the Security Operations domain of SY0-701#6:Chapter 11 CompTIA Security+ Study Guide#.

NEW QUESTION: 237

Which of the following would enable a data center to remain operational through a multiday power outage?

A. Generator

B. Uninterruptible power supply

C. Replication

D. Parallel processing

Answer: (SHOW ANSWER)

The correct answer is A. Generator.

A generator can provide long-term backup power during an extended power outage, as long as sufficient fuel is available. For a multiday outage, a generator is the appropriate solution to keep a data center operational.

This aligns with CompTIA Security+ SY0-701 availability and resilience concepts. Data centers often use generators, redundant power feeds, UPS systems, and environmental controls to maintain uptime.

Why the other options are incorrect:

B . Uninterruptible power supply

A UPS provides short-term backup power and protects against brief outages, power fluctuations, and brownouts. It is usually designed to keep systems running until generator power starts or until systems can be shut down safely.

C . Replication

Replication copies data or systems to another location or system. It supports disaster recovery and availability, but it does not keep the same data center powered during an outage.

D . Parallel processing

Parallel processing distributes computing tasks across multiple processors or systems. It does not provide backup power.

Therefore, a generator is the best answer for a multiday power outage.

NEW QUESTION: 238

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. Phishing campaign

D. Access badges

Answer: (SHOW ANSWER)

NEW QUESTION: 239

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: (SHOW ANSWER)

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.
Reference =
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: 240

Freecram.net

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. Failover site
B. Hot site
C. Warm site
D. Cold site
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which of the following data recovery strategies will result in a quick recovery at low cost?
A. Hot
B. Cold
C. Manual
D. Warm
Answer: D (LEAVE A REPLY)
A warm site offers a compromise between cost and recovery speed. It includes hardware and network infrastructure partially configured, allowing quicker recovery than a cold site but at lower cost than a hot site.
Hot sites (A) enable rapid recovery but at high cost. Cold sites (B) are low cost but slow to recover. Manual (C) refers to manual processes, typically slower.
Warm sites balance recovery time and cost in disaster recovery planning#6:Chapter 9 CompTIA Security+ Study Guide#.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 242
An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?
A. Tokenization
B. Hashing

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

NEW QUESTION: 243
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.Reference: CompTIA SY0-701 Course Content.

NEW QUESTION: 244
Alerts from email protection systems and MSSPs must be entered into an IT service management system and assigned to the security team. Which of the following should an organization implement to enable this functionality?
A. Automated compliance monitoring
B. Automated ticket creation
C. Automated vulnerability scans
D. Automated indicator sharing
Answer: (SHOW ANSWER)
The best answer is B. Automated ticket creation.
The requirement is to take alerts from email protection systems and MSSPs and ensure they are entered into an IT service management system and assigned to the security team. That function is best achieved through automated ticket creation, which generates incidents or service tickets based on incoming alerts and routes them to the appropriate group.
This improves consistency, response time, and tracking of security events.
Why the other options are incorrect:
A). Automated compliance monitoringThis focuses on compliance status, not routing alerts into an ITSM workflow.
C). Automated vulnerability scansVulnerability scanning identifies weaknesses, but it does not create or assign incident tickets from security alerts.
D). Automated indicator sharingIndicator sharing helps distribute threat intelligence, but it does not directly create and assign IT service tickets.
From a Security+ viewpoint, integrating alert sources with response workflows commonly involves ticketing automation, so B is correct.

NEW QUESTION: 245
Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?

A. Honeypot
B. Layer 3 switch
C. IDS
D. Firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 246
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: 247
An organization has been experiencing issues with deleted network share data and improperly assigned permissions. Which of the following would best help track and remediate these issues?
A. DLP
B. EDR
C. FIM
D. ACL
Answer: (SHOW ANSWER)
File Integrity Monitoring (FIM) is the best tool for detecting unauthorized file deletions, modifications, or improper permission changes within network shares. FIM works by creating cryptographic hashes and baselines for protected files or directories and then continuously monitoring for deviations. Any unauthorized deletion, modification, or permission change triggers alerts.

Security+ SY0-701 identifies FIM as a foundational integrity control used in compliance frameworks (PCI- DSS, HIPAA) and operational security monitoring. Because the organization is experiencing unpredictable changes to shared files and permissions, FIM provides visibility and accountability for who changed what and when.
DLP (A) prevents data leakage but does not detect permission changes. EDR (B) focuses on endpoint threat behavior, not file integrity on network shares. ACLs (D) define permissions but do not track changes or detect unauthorized modifications.
Therefore, C: FIM is the correct choice.

NEW QUESTION: 248
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

NEW QUESTION: 249
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?
A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length
Answer: (SHOW ANSWER)
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server. Reference: 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: 250
Which of the following best describe why a process would require a two-person integrity security control?
Freecram.net
A. To Increase the chance that the activity will be completed in half of the time the process would take only one user to complete

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

NEW QUESTION: 251
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. Encryption
B. Data masking
C. Obfuscation
D. Tokenization
Answer: (SHOW ANSWER)

NEW QUESTION: 252
In which of the following will unencrypted PLC management traffic most likely be found?
A. SDN
B. IoT
C. VPN
D. SCADA
Answer: (SHOW ANSWER)
SCADA (Supervisory Control and Data Acquisition) systems commonly manage industrial equipment, including PLCs (Programmable Logic Controllers). Historically, SCADA environments often lack encryption for management traffic due to legacy equipment and protocols. This makes SCADA the most likely environment where unencrypted PLC management traffic can be observed.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2, "SCADA systems often transmit management traffic for PLCs without encryption, making them susceptible to interception." Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

NEW QUESTION: 253
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. Reference: 3: Telnet Protocol - Can You Encrypt Telnet?

NEW QUESTION: 254
An employee decides to collect PII data from the company's system for personal use. The employee compresses the data into a single encrypted file before sending the file to their personal email. The security department becomes aware of the attempted misuse and blocks the attachment from leaving the corporate environment. Which of the following types of employee training would most likely reduce the occurrence of this type of issue?
(Select two).
A. Privacy legislation
B. Social engineering
C. Risk management
D. Company compliance
E. Phishing
F. Remote work
Answer: (SHOW ANSWER)
The misuse of personally identifiable information (PII) is often mitigated through employee training on privacy legislation and company compliance. Training on privacy legislation educates employees about legal requirements and consequences related to handling PII, such as GDPR or HIPAA. Company compliance training reinforces internal policies and procedures regarding data handling, acceptable use, and the repercussions of violations. While social engineering and phishing training are important for security awareness, they address external threats rather than insider misuse of data. Risk management is a broader discipline focused on assessing and mitigating organizational risks but does not directly prevent employee misuse through training. Remote work training focuses on secure practices for working outside corporate environments, which is not the core issue here.
This approach aligns with Security Program Management and Oversight principles emphasizing compliance and privacy training to reduce insider threats#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 255

The Chief Information Officer (CIO) asked a vendor to provide documentation detailing the specific objectives within the compliance framework that the vendor's services meet. The vendor provided a report and a signed letter stating that the services meet 17 of the 21 objectives. Which of the following did the vendor provide to the CIO?

A. Attestation of compliance

B. Penetration test results

C. Self-assessment findings

D. Third-party audit report

Answer: A (LEAVE A REPLY)

NEW QUESTION: 256

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. Introduce a campaign to recognize phishing attempts.

C. Implement a deny list of websites.

D. Restrict internet access for the employees who disclosed credentials.

Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 257

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: 258

A company is concerned about the theft of client data from decommissioned laptops. Which of the following is the most cost-effective method to decrease this risk?

A. Wiping

B. Recycling

C. Shredding

D. Deletion

Answer: (SHOW ANSWER)

Wiping involves securely erasing data by overwriting the hard drive, ensuring the information is unrecoverable. It is cost-effective compared to physical destruction methods like shredding.

NEW QUESTION: 259

Which of the following should a technician perform to verify the integrity of a file transferred from one device to another?

A. Authentication

B. Obfuscation

C. Hashing

D. Encryption

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From Exact Extract:

Hashing is the process used to verify file integrity. When transferring a file between devices, a hash value (such as SHA-256) is generated before the transfer and then recomputed afterward. If the two hash values match, the file has not been altered, corrupted, or tampered with during transmission. Authentication (A) verifies identity, not file integrity. Obfuscation (B) hides meaning but does not detect modification. Encryption (D) protects confidentiality but does not guarantee integrity unless combined with hashing or digital signatures.

CompTIA Security+ SY0-701 covers hashing under cryptographic functions used for integrity verification. Hash algorithms ensure that even a single byte change results in a completely different hash value (the avalanche effect). This makes hashing the standard method for verifying the integrity of transferred files, software downloads, backups, and system images.

NEW QUESTION: 260

Which of the following will harden access to a new database system? (Select two)

A. Jump server

B. NIDS

C. Monitoring

D. Proxy server

E. Host-based firewall

F. WAF

Answer: (SHOW ANSWER)

Hardening access to a new database system requires implementing controls that restrict and secure how administrators and applications connect to the database. A jump server (A) is a hardened intermediary system used to manage access to sensitive systems such as databases. By forcing administrators to authenticate through a controlled, monitored jump host instead of connecting directly, organizations reduce attack surfaces and prevent unauthorized lateral movement. Security+ SY0-701 identifies jump servers as critical in securing high-value systems.

A host-based firewall (E) provides system-level traffic filtering directly on the database server. It allows only trusted IPs, ports, and services to communicate with the database, significantly reducing exposure. This is an essential hardening measure because databases should only accept

connections from specific application servers or administrative hosts.
NIDS (B) monitors traffic but does not harden access. Monitoring (C) provides visibility but does not restrict access. A proxy server (D) is not typically used for database access. A WAF (F) protects web applications, not internal database systems.
Thus, A (Jump server) and E (Host-based firewall) are the correct hardening controls.

NEW QUESTION: 261
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: 262
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.
Reference:
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: 263
A security administrator protects passwords by using hashing. Which of the following best describes what the administrator is doing?
A. Adding extra characters at the end to increase password length
B. Generating a token to make the passwords temporal

C. Using mathematical algorithms to make passwords unique
D. Creating a rainbow table to protect passwords in a list
Answer: (SHOW ANSWER)
Hashing is the process of converting plaintext passwords into a fixed-length, irreversible string using a mathematical algorithm (hash function). This makes each password unique based on its content, and even a small change in the password will produce a different hash. The primary purpose is to ensure that the actual passwords are not stored directly and cannot be easily recovered from the hash, even if the hash is compromised.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Hashing ensures that plaintext passwords are not stored directly. Hash functions use mathematical algorithms to produce unique, fixed-length output for each unique input." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

NEW QUESTION: 264
A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team. Which of the following should the company implement to meet this requirement?
A. VDI
B. MDM
C. VPN
D. VPC
Answer: (SHOW ANSWER)
Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server. Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company's infrastructure without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company's secure servers.
Reference =
CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

NEW QUESTION: 265
A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?
A. Certification
B. Inventory list
C. Classification
D. Proof of ownership
Answer: (SHOW ANSWER)
The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

NEW QUESTION: 266

Which of the following architectures is most suitable to provide redundancy for critical business processes?
A. Network-enabled
B. Cloud-native
C. Multitenant
D. Server-side
Answer: (SHOW ANSWER)

NEW QUESTION: 267
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: (SHOW ANSWER)
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: 268
After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?
A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling
Answer: (SHOW ANSWER)
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

NEW QUESTION: 269
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: (SHOW ANSWER)

Detailed 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: 270

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: 271

As part of new compliance audit requirements, multiple servers need to be segmented on different networks and should be reachable only from authorized internal systems. Which of the following would meet the requirements?

A. Configure firewall rules to block external access to Internal resources.

B. Set up a WAP to allow internal access from public networks.

C. Implement a new IPSec tunnel from internal resources.

D. Deploy an Internal Jump server to access resources.

Answer: (SHOW ANSWER)

"Network segmentation is a security practice that divides a network into smaller, isolated segments to limit access and reduce the attack surface. Firewalls are commonly used to enforce segmentation by creating rules that allow or deny traffic based on source, destination, and port. Tomeet compliance requirements, such as restricting access to internal servers, firewall rules can be configured to block all external traffic while permitting only authorized internal systems to communicate with the segmented servers. This ensures that sensitive resources are isolated from unauthorized access."

Reference:

The requirement is to segment servers on different networks and restrict access to only authorized internal systems. Option A directly addresses this by using firewall rules to block external access while allowing internal traffic, aligning with network segmentation best practices. Option B (WAP) refers to a Wireless Access Point, which doesn't fit the context of segmentation and could expose resources to public networks. Option C (IPSec tunnel) secures communication but doesn't inherently segment networks. Option D (jump server) adds a layer of access control but doesn't address the segmentation

requirement alone. Thus, A is the best fit.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 272
A security analyst has determined that a security breach would have a financial impact of $15,000 and is expected to occur twice within a three-year period. Which of the following is the ALE for this risk?
A. $30,000
B. $15,000
C. $10,000
D. $7,500
Answer: (SHOW ANSWER)

NEW QUESTION: 273
The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced faded log-In attempts when authenticating from the same IP address:

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

Which of the following most likely describes attack that took place?
A. Dictionary
B. Brute-force
C. Spraying
D. Rainbow table
Answer: (SHOW ANSWER)

NEW QUESTION: 274
An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?
A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls
Answer: D (LEAVE A REPLY)
Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded

services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.
Reference:
Official CompTIA Security+ Study Guide (SY0-701), page 29
Security Controls - CompTIA Security+ SY0-701 - 1.1 1

NEW QUESTION: 275
Which of the following alert types is the most likely to be ignored over time?
A. True positive
B. True negative
C. False positive
D. False negative
Answer: (SHOW ANSWER)
A false positive is an alert that incorrectly identifies benign activity as malicious. Over time, if an alerting system generates too many false positives, security teams are likely to ignore these alerts, resulting in "alert fatigue." This increases the risk of missing genuine threats.
True positives and true negatives are accurate and should be acted upon.
False negatives are more dangerous because they fail to identify real threats, but they are not "ignored" since they do not trigger alerts.

NEW QUESTION: 276
A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?
A. Serverless architecture
B. Thin clients
C. Private cloud
D. Virtual machines
Answer: (SHOW ANSWER)
Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance. Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.
Reference =
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: 277
A penetration test has demonstrated that domain administrator accounts were vulnerable to pass-the-hash attacks. Which of the following would have been the best strategy to prevent the threat actor from using domain administrator accounts?
A. Audit each domain administrator account weekly for password compliance.
B. Implement a privileged access management solution.
C. Create IDS policies to monitor domain controller access.
D. Use Group Policy to enforce password expiration.
Answer: (SHOW ANSWER)
Detailed Privileged access management (PAM) solutions effectively mitigate pass-the-hash attacks by enforcing least privilege and session management for administrative accounts. These tools restrict how and when credentials can be accessed, thereby reducing attack surfaces. Reference: CompTIA

Security+ SY0-701 Study Guide, Domain 2: Vulnerabilities, Section: "Mitigation Techniques".

NEW QUESTION: 278
A marketing team launches a new AI solution that trains on sensitive customer data to help provide recommendations on its next possible marketing campaign. This team requires granular access to the tool for different levels of sensitive data. Which of the following should a systems administrator prioritize when provisioning access?
A. Emergency access
B. Least-privilege accounts
C. Just-in-time (JIT) access
D. Group managed service accounts
Answer: (SHOW ANSWER)
Least-privilege accounts are the correct choice because the scenario requires granular access to different levels of sensitive customer data. The principle of least privilege ensures users receive only the minimum permissions required to perform their job duties and nothing more. This is especially important when AI tools process sensitive data, because excessive access can expose regulated, private, or confidential information to unauthorized users. Emergency access is reserved for break-glass situations and should not be the normal provisioning model. Just-in-time access is useful for temporary privileged access, but the question emphasizes ongoing granular access levels. Group managed service accounts are used for service authentication, not user access to sensitive AI data. Least privilege best aligns with secure access provisioning.

NEW QUESTION: 279
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: (SHOW ANSWER)
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: 280
A service provider wants a cost-effective way to rapidly expand from providing internet links to managing them. Which of the following methods will allow the service provider to best scale its services while maintaining performance consistency?
Freecram.net
A. Escalation support
B. Increased workforce
C. Baseline enforcement
D. Technical debt
Answer: (SHOW ANSWER)
Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently

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

NEW QUESTION: 281
Which of the following best protects sensitive data in transit across a geographically dispersed Infrastructure?
A. Obfuscation
B. Masking
C. Encryption
D. Tokenization
Answer: (SHOW ANSWER)

NEW QUESTION: 282
A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?
A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.
Answer: (SHOW ANSWER)
The next step should be to rescan the network. In vulnerability management, remediation is not complete simply because the operations team says fixes were applied. The security team must validate that the vulnerabilities are actually resolved. A rescan confirms whether patches, configuration changes, service removals, or compensating controls eliminated the previously identified weaknesses. Conducting an audit is broader and not the immediate technical validation step. Starting a penetration test may be useful later, but it is unnecessary before confirming that the known vulnerabilities were fixed. Submitting a report before validation could produce inaccurate closure information. Security+ expects vulnerability management to follow a cycle: identify, analyze, remediate, validate, and report. Validation is done through rescanning.

NEW QUESTION: 283
Sine a recent upgrade (o a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings. Which of the following installation considerations should the security team evaluate next?
A. Channel overlap
B. Encryption type
C. New WLAN deployment
D. WAP placement
Answer: A (LEAVE A REPLY)
When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting

the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.
Reference = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

NEW QUESTION: 284
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: (SHOW ANSWER)
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.
Reference =
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: 285
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?
A. Real-time recovery
B. Hot
C. Cold
D. Warm
Answer: (SHOW ANSWER)
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. Reference = CompTIA Security + SY0-701 Certification Study Guide, page 387; Backup Types - SY0-601 CompTIA Security+ : 2.5, video at 4:50.

NEW QUESTION: 286
An external vendor recently visited a company's headquarters tor a presentation. Following the visit a member of the hosting team found a file that the external vendor left behind on a server. The file contained detailed architecture information and code snippets. Which of the following data types best describes this file?
A. Government
B. Public
C. Proprietary
D. Critical

Answer: (SHOW ANSWER)
The file left by the external vendor, containing detailed architecture information and code snippets, is best described as proprietary data. Proprietary data is information that is owned by a company and is essential to its competitive advantage. It includes sensitive business information such as trade secrets, intellectual property, and confidential data that should be protected from unauthorized access.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of data classification and protection.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 287
Following a security review, an organization must ensure users verify their identities against the company's identity services with individual credentials leveraging WPA2-Enterprise for wireless access. Which of the following configuration steps correctly applies RADIUS in this environment?
A. Enabling 802.1X authentication and integrating it with the corporate directory
B. Installing self-signed certificates on all user devices
C. Enabling MAC filters for all wireless clients
D. Configuring the wireless controller to require multifactor authentication
Answer: (SHOW ANSWER)
WPA2-Enterprise is designed for environments where users authenticate with unique, individual credentials backed by an enterprise identity store, rather than a shared preshared key. The Study Guide explicitly states: "WPA2-Enterprise relies on a RADIUS authentication server as part of an 802.1X implementation for authentication. Users can thus have unique credentials and be individually identified." That maps directly to the requirement that users verify identity against the company's identity services using individual credentials. It further explains how this is implemented operationally: "802.1X is an IEEE standard for access control... In wireless networks, 802.1X is used to integrate with RADIUS servers, allowing enterprise users to authenticate and gain access to the network." Therefore, the correct configuration step is enabling 802.1X and tying authentication into the organization's identity source (commonly a corporate directory). The other choices don't correctly "apply RADIUS" for WPA2-Enterprise: self-signed certs are not universally required for all EAP types and can introduce trust issues; MAC filters are weak and spoofable; and MFA might be beneficial but is not the fundamental step that enables RADIUS-backed WPA2-Enterprise authentication.

NEW QUESTION: 288
A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach end does not have an on-premises IT infrastructure. Which of the following would best secure the organization?
A. Upgrading to a next-generation firewall
B. Deploying an appropriate in-line CASB solution
C. Conducting user training on software policies
D. Configuring double key encryption in SaaS platforms
Answer: (SHOW ANSWER)
A Cloud Access Security Broker (CASB) solution is the most suitable option for securing an organization that has adopted a cloud-first strategy and does not have an on-premises IT infrastructure. CASBs provide visibility and control over shadow IT services, enforce security policies, and protect data across cloud services.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of cloud security and managing risks associated with shadow IT.

NEW QUESTION: 289
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: (SHOW ANSWER)
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

NEW QUESTION: 290
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?
Freecram.net
A. Serverless framework
B. Type 1 hypervisor
C. SD-WAN
D. SDN
Answer: (SHOW ANSWER)
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.
SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

Reference = 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: 291
An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?
A. Asset inventory
B. Network enumeration
C. Data certification
D. Procurement process
Answer: (SHOW ANSWER)
To ensure that all systems requiring the patch are updated, the systems administrator must maintain an accurate asset inventory. This inventory lists all hardware and software assets within the organization, allowing the administrator to identify which systems are affected by the patch and ensuring that none are missed during the update process.
* Network enumeration is used to discover devices on a network but doesn't track software that requires patching.
* Data certification and procurement process are unrelated to tracking systems for patching purposes.

NEW QUESTION: 292
The Chief Information Security Officer (CISO) of a medium-sized business plans to modernize the existing security infrastructure and address issues with legacy software and assets. Which of the following should the CISO use to determine the scope of the legacy infrastructure and develop a risk-based approach to modernization?
A. Angry IP Scanner
B. OWASP Web Security Testing Guide
C. CIS benchmarks
D. Metasploit Framework
Answer: (SHOW ANSWER)
CIS benchmarks are the best choice because they provide recognized secure configuration baselines for operating systems, applications, cloud platforms, network devices, and other infrastructure components. A CISO modernizing legacy systems needs a structured way to evaluate current configurations, identify gaps, prioritize weaknesses, and build a risk-based remediation plan. Angry IP Scanner can help discover live hosts, but it does not provide security baselines or modernization guidance. The OWASP Web Security Testing Guide focuses on web application testing, not broad legacy infrastructure. Metasploit is a penetration testing framework and is not the right tool for defining modernization scope. Security+ emphasizes secure baselines, hardening standards, and benchmark-driven configuration review for reducing risk.

NEW QUESTION: 293
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: 294
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?
A. Virus
B. Trojan
C. Spyware
D. Ransomware
Answer: (SHOW ANSWER)
Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.

NEW QUESTION: 295
Which of the following is an example of implementing Zero Trust architecture?
A. Building strong network boundaries to prevent intrusion
B. Verifying user identity once at the start of the session
C. Granting resource access after continuous validation
D. Prioritizing perimeter defense to block external threats
Answer: (SHOW ANSWER)
The best answer is C. Granting resource access after continuous validation.
Zero Trust architecture is based on the principle of never trust, always verify. Access should not be granted simply because a user or device is inside the network or was authenticated once earlier. Instead, access decisions should be based on continuous validation of identity, device health, context, and other relevant factors.
This means users and devices are evaluated repeatedly and granted only the minimum access necessary.
Why the other options are incorrect:
A). Building strong network boundaries to prevent intrusionThis reflects a traditional perimeter-based security model, not Zero Trust.
B). Verifying user identity once at the start of the sessionZero Trust does not rely on one-time authentication alone. It emphasizes ongoing verification.
D). Prioritizing perimeter defense to block external threatsAgain, this focuses on perimeter security rather than continuous, identity- and context-based access control.
From a Security+ perspective, Zero Trust is best represented by continuous validation before and during access, which makes C correct.

NEW QUESTION: 296
A customer of a large company receives a phone call from someone claiming to work for the company and asking for the customer's credit card information. The customer sees the caller ID is the same as the company's main phone number. Which of the following attacks is the customer most likely a target of?
A. Vishing

B. Smishing
C. Whaling
D. Phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Which of the following should be used to ensure a device is inaccessible to a network-connected resource?
A. Disablement of unused services
B. Web application firewall
C. Host isolation
D. Network-based IDS
Answer: (SHOW ANSWER)
Detailed Host isolation ensures that a device is separated from the network, preventing it from accessing or being accessed by other network resources. This is typically achieved by quarantining the device. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Isolation and Containment".

NEW QUESTION: 298
Which of the following must be considered when designing a high-availability network? (Select two).
A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication
Answer: (SHOW ANSWER)
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.
Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.
Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

NEW QUESTION: 299
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?
A. Clustering servers
B. Geographic dispersion

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

NEW QUESTION: 300
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?
Freecram.net
A. Load balancer
B. Port security
C. IPS
D. NGFW
Answer: (SHOW ANSWER)
Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.
Load balancer distributes network traffic but does not address MAC flooding attacks.
IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.
NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC table security.

NEW QUESTION: 301
An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).
A. Application
B. Authentication
C. DHCP

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

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 302
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: 303

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: (SHOW ANSWER)

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: 304

A security analyst notices an increase in port scans on the edge of the corporate network. Which of the following logs should the analyst check to obtain the attacker's source IP address?

A. Security

B. Firewall

C. Application

D. Endpoint

Answer: (SHOW ANSWER)

Firewall logs are the best source for identifying the attacker's source IP address during port scanning activity at the network edge. A firewall sits at or near the boundary between trusted and untrusted networks and records traffic attempts, including source IP, destination IP, protocol, port, action taken, and timestamps. Since the scans are occurring on the edge of the corporate network, firewall telemetry is the most relevant data source. Security logs usually refer to operating system authentication or authorization events, not perimeter scan traffic. Application logs record application-level behavior and errors. Endpoint logs are useful for host activity, processes, and local connections, but the question specifically points to edge scanning. Therefore, firewall logs are the correct operational source.

NEW QUESTION: 305

Which of the following is the most likely motivation for a hacktivist?

A. Financial gain

B. Service disruption

C. Philosophical beliefs

D. Corporate espionage

Answer: (SHOW ANSWER)

Hacktivists are individuals or groups who use hacking to promote a political agenda, social cause, or philosophical beliefs. Their primary motivation is not personal gain but rather to draw attention to, or protest against, perceived injustices or causes.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Hacktivists are motivated by ideology or political/social causes." Exam Objectives 2.1: "Compare and contrast different types of threat actors."

NEW QUESTION: 306

The management team reports employees are missing features on company-provided tablets, causing productivity issues. The team directs IT to resolve the issue within 48 hours. Which of the following is the best solution?

A. EDR

B. COPE

C. MDM

D. FDE

Answer: (SHOW ANSWER)

The best solution is Mobile Device Management (MDM), which allows IT administrators to centrally configure, update, and push applications or settings to company-owned devices. When employees report missing features or misconfigurations, MDM platforms enable rapid remote remediation, policy enforcement, patch distribution, and application deployment-all of which can be completed within the 48-hour requirement.

Security+ SY0-701 emphasizes MDM as the primary tool for ensuring consistent configuration baselines, enforcing security restrictions, deploying apps, and preventing unauthorized changes on mobile devices.

EDR (A) provides threat detection, not configuration restoration.

COPE (B) is a device ownership model (Corporate Owned, Personally Enabled); it does not solve configuration issues.

FDE (D) encrypts storage, unrelated to missing features.

Therefore, C: MDM is the correct answer.

NEW QUESTION: 307

A security analyst investigates abnormal outbound traffic from a corporate endpoint. The traffic is encrypted and uses non-standard ports. Which of the following data sources should the analyst use first to confirm whether this traffic is malicious?

A. Application logs

B. Vulnerability scans

C. Endpoint logs

D. Packet captures

Answer: (SHOW ANSWER)

When investigating abnormal outbound traffic originating from a specific endpoint, endpoint logs are the most appropriate first data source to review. According to CompTIA Security+ SY0-701, endpoint logs provide detailed visibility into process execution, user actions, service creation, network connections initiated by applications, and security agent detections. This context is critical for determining which process initiated the encrypted traffic and why it is using non-standard ports.

Because the traffic is encrypted, packet captures (D) would reveal limited payload information and are more resource-intensive. Endpoint logs can quickly identify suspicious executables, command-line arguments, parent-child process relationships, and persistence mechanisms that indicate malware or command-and- control activity. Modern EDR tools rely heavily on endpoint telemetry for exactly this reason.

Application logs (A) may be useful later but are limited to specific applications. Vulnerability scans (B) identify weaknesses, not active malicious behavior.

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

NEW QUESTION: 308

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: (SHOW ANSWER)
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. Reference = CompTIA Security+ SY0-701 study materials, particularly on incident response procedures and the importance of containment in managing security incidents.

NEW QUESTION: 309
A company wants to track modifications to the code used to build new virtual servers. Which of the following will the company most likely deploy?
A. Change management ticketing system
B. Behavioral analyzer
C. Collaboration platform
D. Version control tool
Answer: D (LEAVE A REPLY)
Detailed 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: 310
An analyst wants to move data from production to the UAT server to test the latest release. Which of the following strategies should the analyst use to protect sensitive data from being viewed by the testing team?
Freecram.net
A. Data masking
B. Data tokenization
C. Data obfuscation
D. Data encryption
Answer: (SHOW ANSWER)
The best answer is A. Data masking.
When production data is copied into a UAT (User Acceptance Testing) environment, sensitive information should be protected so that testers cannot view real confidential values such as personal data, account numbers, or other regulated information. Data masking replaces sensitive data with realistic but fictional or hidden values while preserving the format and usability of the data for testing.
This makes it ideal for non-production environments where the application still needs data that looks real, but the testing team should not be able to see actual sensitive information.
Why the other options are incorrect:
B). Data tokenizationTokenization replaces sensitive values with tokens, but it is more commonly used to protect data in operational processing systems, such as payment environments. It is not the best fit here compared with masking for UAT visibility concerns.
C). Data obfuscationObfuscation is a broader term and can mean making data harder to understand, but data masking is the more precise and standard control for protecting test data from being viewed.
D). Data encryptionEncryption protects data at rest or in transit, but once authorized testers access and use the UAT system, the application may decrypt and display the data. That does not solve the problem of testers viewing sensitive values.
From a Security+ perspective, when moving production data into development, test, or UAT environments, the preferred control to prevent exposure of

real sensitive data is data masking.

NEW QUESTION: 311
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
. Something you know
. Something you are
: Something you have
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: (SHOW ANSWER)
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.
Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12 Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12 Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12 Reference:
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: 312
An administrator is reviewing a single server's security logs and discovers the following; Which of the following best describes the action captured in this log file?
A. Brute-force attack
B. Privilege escalation
C. Failed password audit
D. Forgotten password by the user
Answer: (SHOW ANSWER)
A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

NEW QUESTION: 313
Which of the following methods would most likely be used to identify legacy systems?
A. Bug bounty program
B. Vulnerability scan

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

NEW QUESTION: 314
A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?
A. Host-based firewall
B. Web application firewall
C. Access control list
D. Application allow list
Answer: (SHOW ANSWER)
A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

NEW QUESTION: 315
Which of the following best explains the role of compensating controls?
A. Reducing the attack surface by isolating vulnerable components within a segmented environment
B. Providing an alternative security measure when standard remediation is not feasible
C. Delaying remediation timelines by replacing affected systems in a maintenance window
D. Remediating software flaws by modifying source code to remove insecure functions
Answer: (SHOW ANSWER)
The best answer is B. Providing an alternative security measure when standard remediation is not feasible.
A compensating control is a substitute safeguard used when the preferred or required control cannot be implemented immediately or at all. It helps reduce risk in another way until proper remediation is possible, or when direct remediation is impractical.
Examples include:
increasing monitoring when a system cannot be patched
segmenting a legacy application that cannot be upgraded
restricting access to a vulnerable system that must remain in service
Why the other options are incorrect:

A). Reducing the attack surface by isolating vulnerable components within a segmented environmentThis can be an example of a compensating control, but it does not define the overall role as clearly as B.
C). Delaying remediation timelines by replacing affected systems in a maintenance windowThis describes scheduling or change timing, not compensating controls.
D). Remediating software flaws by modifying source code to remove insecure functionsThis is direct remediation, not a compensating control.
From the SY0-701 perspective, compensating controls are used when the ideal fix is not possible, so B is the best explanation.

NEW QUESTION: 316
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?
A. Accept
B. Transfer
C. Mitigate
D. Avoid
Answer: (SHOW ANSWER)
Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:
Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.
Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.
Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.
Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.
By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B. Transfer. Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 317
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: (SHOW ANSWER)

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.

NEW QUESTION: 318

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: (SHOW ANSWER)

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.

NEW QUESTION: 319

Which of the following is the best method to reduce the attack surface of an enterprise network?

A. Create a guest wireless network for visitors.
B. Disable unused network services on servers.
C. Use port security for wired connections.
D. Change default passwords for network printers.

Answer: (SHOW ANSWER)

NEW QUESTION: 320

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

Freecram.net

A. Code scanning for vulnerabilities

B. Open-source component usage

C. Quality assurance testing

D. Peer review and approval

Answer: (SHOW ANSWER)

The correct answer is D. Peer review and approval.

Peer review and approval help prevent a single developer or insider from inserting malicious code without oversight. This practice supports separation of duties, accountability, secure software development, and change control. Requiring another qualified person to review and approve code changes increases the chance that suspicious, unauthorized, or malicious code will be identified before it enters production.

Why the other options are incorrect:

A . Code scanning for vulnerabilities

Code scanning can identify known vulnerabilities, insecure coding patterns, and some misconfigurations. However, malicious code intentionally written to appear legitimate may not always be detected by automated scanning.

B . Open-source component usage

Using open-source components does not prevent insider abuse. In fact, open-source dependencies may introduce additional supply chain risk if not properly reviewed.

C . Quality assurance testing

Quality assurance testing verifies whether software works as intended, but it may not detect intentionally malicious logic hidden in the code.

Therefore, peer review and approval is the best practice to prevent an insider from introducing malicious code into the development process.

NEW QUESTION: 321

An organization determines that tenured employees have retained privileges beyond those required to perform their duties. Which of the following should the organization do to address the issue?

A. Implement regular account reviews.

B. Provide privileged user account training.

C. Require a jump box for privileged account use.

D. Apply more restrictive security baselines.

Answer: (SHOW ANSWER)

The correct answer is A. Implement regular account reviews.

This scenario describes privilege creep, which occurs when users accumulate permissions over time as they change roles, departments, or responsibilities. Regular account reviews help ensure users have only the access required for their current job duties.

This supports the principle of least privilege, which is a key CompTIA Security+ SY0-701 identity and access management concept.

Why the other options are incorrect:

B . Provide privileged user account training

Training is useful, but it does not remove unnecessary privileges.

C . Require a jump box for privileged account use

A jump box can control administrative access to sensitive systems, but it does not solve the issue of users retaining excessive privileges.

D . Apply more restrictive security baselines

Security baselines harden systems and configurations, but they do not directly review or remove unnecessary user permissions.

Therefore, the best answer is regular account reviews.

NEW QUESTION: 322

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: (SHOW ANSWER)

NEW QUESTION: 323

Which of the following most accurately describes the order in which a security engineer should implement secure baselines?

A. Deploy, maintain, establish

B. Establish, maintain, deploy

C. Establish, deploy, maintain

D. Deploy, establish, maintain

Answer: (SHOW ANSWER)

Detailed The correct sequence is to first establish secure baselines by determining the required configurations, deploy those configurations across systems, and finally maintain the configurations through regular updates and auditing. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Secure Baseline Development".

NEW QUESTION: 324

Which of the following would be the greatest concern for a company that is aware of the consequences of non-compliance with government regulations?

A. Right to be forgotten

B. Sanctions

C. External compliance reporting

D. Attestation

Answer: B (LEAVE A REPLY)

Detailed

Sanctions imposed for non-compliance can include fines, legal actions, and loss of business licenses. These pose a significant financial and reputational risk to organizations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Regulatory Compliance Risks".

NEW QUESTION: 325

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)

Input validationensures 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 activelypreventinjection attacks in real- time.
Implementingstrong input validationcanprevent malicious code from being executed, reducing the risk of injection attacks.

NEW QUESTION: 326
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.

NEW QUESTION: 327
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: (SHOW ANSWER)
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 and spear-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.
Reference1: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

NEW QUESTION: 328
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: (SHOW ANSWER)
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: 329
A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?
A. Insurance
B. Patching
C. Segmentation
D. Replacement
Answer: (SHOW ANSWER)
Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

NEW QUESTION: 330
During a routine audit, an analyst discovers that a department uses software that was not vetted. Which threat is this?
Freecram.net

A. Espionage
B. Data exfiltration
C. Shadow IT
D. Zero-day
Answer: (SHOW ANSWER)
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: 331
A security administrator wants to implement a security information and event management system. The administrator must first collect network traffic on the switch to gain visibility of the network. Which of the following is the most appropriate method?
A. Syslog
B. Port mirroring
C. Port forwarding
D. Load balancer logs
Answer: (SHOW ANSWER)
The correct answer is B. Port mirroring.
Port mirroring, also known as SPAN, copies network traffic from one or more switch ports or VLANs to another port where a monitoring tool, packet analyzer, IDS, or SIEM-related sensor can inspect the traffic. This is the most appropriate method when the goal is to collect network traffic directly from a switch to gain visibility into network activity.
Why the other options are incorrect:
A . Syslog
Syslog collects log messages from systems, applications, and network devices. It is useful for SIEM log ingestion, but it does not capture full network traffic from a switch.
C . Port forwarding
Port forwarding redirects traffic from one port or IP address to another, commonly used for NAT or remote access. It is not used to monitor switch traffic.
D . Load balancer logs
Load balancer logs provide information about traffic passing through a load balancer, but they do not provide broad switch-level network visibility.
Therefore, the best answer is port mirroring.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 332
Which of the following elements of digital forensics should a company use If It needs to ensure the integrity of evidence?
A. Acquisition
B. Preservation
C. E-discovery
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 333
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

NEW QUESTION: 334
Which of the following is an example of memory injection?
A. A process receives an unexpected amount of data, which causes malicious code to be executed.
B. Malicious code is copied to the allocated space of an already running process.
C. Two processes access the same variable, allowing one to cause a privilege escalation.
D. An executable is overwritten on the disk, and malicious code runs the next time it is executed.
Answer: (SHOW ANSWER)

NEW QUESTION: 335
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: (SHOW ANSWER)
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: 336
Which of the following can be used to compromise a system that is running an RTOS?
A. Cross-site scripting
B. Memory injection
C. Replay attack
D. Ransomware
Answer: (SHOW ANSWER)
The correct answer is B. Memory injection.
An RTOS, or real-time operating system, is commonly used in embedded systems, industrial systems, medical devices, vehicles, and operational technology environments. These systems often have strict timing requirements and may run specialized software with limited security protections.
Memory injection can be used to compromise systems by inserting malicious code or commands into memory. This can allow an attacker to alter execution flow, manipulate processes, bypass controls, or gain unauthorized control of the device.
Why the other options are incorrect:
A). Cross-site scripting
Cross-site scripting is primarily a web application attack. It is not the best answer for compromising a system running an RTOS.
C). Replay attack
A replay attack captures and retransmits valid data or authentication messages. It may affect some embedded or industrial communication systems, but it does not directly describe compromising the RTOS itself as well as memory injection.
D). Ransomware
Ransomware encrypts or locks data and demands payment. While some embedded systems could theoretically be disrupted by malware, ransomware is not the best match for compromising an RTOS.
Therefore, the best answer is memory injection.

NEW QUESTION: 337
Which of the following allows an exploit to go undetected by the operating system?
A. Encrypted payloads
B. Side loading
C. Memory injection
D. Firmware vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 338
A software developer would like to ensure. The source code cannot be reverse engineered or debugged. Which of the following should the developer consider?
A. Version control

B. Obfuscation toolkit
C. Code reuse
D. Continuous integration
E. Stored procedures
Answer: (SHOW ANSWER)
An obfuscation toolkit is used by developers to make source code difficult to understand and reverse engineer. This technique involves altering the code's structure and naming conventions without changing its functionality, making it much harder for attackers to decipher the code or use debugging tools to analyze it. Obfuscation is an important practice in protecting proprietary software and intellectual property from reverse engineering.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Coding Practices.

NEW QUESTION: 339
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: 340
A business provides long-term cold storage services to banks that are required to follow regulator-imposed data retention guidelines. Banks that use these services require that data is disposed of in a specific manner at the conclusion of the regulatory threshold for data retention. Which of the following aspects of data management is the most important to the bank in the destruction of this data?
Freecram.net
A. Encryption
B. Classification
C. Certification

D. Procurement

Answer: (SHOW ANSWER)

Classification is the process of assigning a level of sensitivity and handling requirements to data, which informs its lifecycle management, retention, and disposal methods. In regulated industries such as banking, proper data classification ensures that data subject to legal or regulatory requirements is destroyed according to those requirements at the end of its retention period. This directly guides how the data should be handled and disposed of.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "Classification dictates data handling, storage, retention, and destruction policies in compliance with regulatory requirements." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

NEW QUESTION: 341

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: (SHOW ANSWER)

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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

NEW QUESTION: 342

Which of the following is the main consideration when a legacy system that is a critical part of a company's infrastructure cannot be replaced?

A. Complexity

B. Cost

C. Single point of failure

D. Resource provisioning

Answer: (SHOW ANSWER)

NEW QUESTION: 343

Which of the following is the first step to take when creating an anomaly detection process?

A. Selecting events

B. Building a baseline

C. Selecting logging options

D. Creating an event log

Answer: B (LEAVE A REPLY)

The first step in creating an anomaly detection process is building a baseline of normal behavior within the system. This baseline serves as a reference point to identify deviations or anomalies that could indicate a security incident. By understanding what normal activity looks like, security teams can more effectively detect and respond to suspicious behavior.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Monitoring and Baselines.

NEW QUESTION: 344
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.
Reference = 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: 345
Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.
Which of the following changes would allow users to access the site?
A. Creating a firewall rule to allow HTTPS traffic
B. Configuring the IPS to allow shopping
C. Tuning the DLP rule that detects credit card data
D. Updating the categorization in the content filter
Answer: (SHOW ANSWER)
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow

access to the website instead of blocking it.

NEW QUESTION: 346
Which of the following tools is best for logging and monitoring in a cloud environment?
A. NAC
B. SIEM
C. IPS
D. FIM
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 347
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?
A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor
Answer: (SHOW ANSWER)
= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. Reference = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances - SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

NEW QUESTION: 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 systems is one of the most effective ways to reduce the attack surface. Unsupported OS versions no longer receive security patches, making them prime targets for attackers. Removing outdated software ensures that known vulnerabilities cannot be exploited.
* A (honeynet) is used for threat analysis, not reducing the attack surface.
* B (Group Policy) helps enforce security policies but does not address outdated vulnerabilities.
* C (High availability) focuses on uptime, not security risk reduction.

NEW QUESTION: 349
Which of the following phases of an incident response involves generating reports?
A. Recovery
B. Preparation
C. Lessons learned
D. Containment
Answer: (SHOW ANSWER)
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: 350
Which of the following is a reason an organization should use different CSPs for a critical financial application?
Freecram.net
A. Application overhead can be better load balanced across multiple providers.
B. Platform diversity reduces the likelihood of losing access to resources.
C. Parallel processing allows continued operations while deploying time-critical security updates.
D. Selection of a hot site minimizes downtime and helps the organization meet its RTO.
Answer: (SHOW ANSWER)
Using different cloud service providers supports platform diversity and reduces dependency on a single provider. For a critical financial application, this improves resilience because a provider outage, regional disruption, account issue, or provider-specific service failure is less likely to make all resources unavailable at once. This is a multi-cloud availability and continuity strategy. Option A focuses on load balancing application overhead, which may be possible but is not the strongest Security+ reason for using different CSPs. Option C incorrectly frames the benefit as parallel processing for security updates. Option D describes a hot site, which is a disaster recovery location, not necessarily the reason for using multiple CSPs. The core architectural benefit is reducing single-provider dependency through platform diversity.

NEW QUESTION: 351
A company wants to use new Wi-Fi-enabled environmental sensors to automatically collect metrics. Which of the following will the security team most likely do?
A. Add the sensor software to the risk register.
B. Create a VLAN for the sensors.
C. Physically air gap the sensors.
D. Configure TLS 1.2 on all sensors.

Answer: (SHOW ANSWER)
Creating a VLAN for Wi-Fi-enabled environmental sensors is the most likely and appropriate action. Security+ SY0-701 recommends network segmentation for IoT and sensor devices to reduce attack surface and limit lateral movement. A dedicated VLAN isolates sensors from critical systems while allowing controlled access to data collectors or management platforms.
Adding items to a risk register (A) documents risk but does not provide protection. Physically air gapping (C) contradicts the requirement for Wi-Fi connectivity. Configuring TLS 1.2 (D) is beneficial for data-in-transit protection but does not address network-level isolation and blast-radius reduction.
Thus, B: Create a VLAN for the sensors best aligns with secure design.

NEW QUESTION: 352
A network engineer is increasing the overall security of network devices and needs to harden the devices. Which of the following will best accomplish this task?
A. Configuring centralized logging
B. Enabling HTTP administration
C. Generating local administrator accounts
D. Replacing Telnet with SSH
Answer: (SHOW ANSWER)

NEW QUESTION: 353
Which of the following best explains a core principle of a Zero Trust security model?
A. Devices connected to the internal network are automatically trusted after initial authentication.
B. Access to resources is granted only after strict identity verification and continuous monitoring.
C. Security policies require multifactor authentication for remote access to sensitive data.
D. Network access is limited by role, and access controls are reviewed on a regular schedule.
Answer: (SHOW ANSWER)
Zero Trust is based on the principle of "never trust, always verify." Option B is correct because access is granted only after strong identity verification, policy evaluation, and continuous monitoring. Zero Trust rejects the old perimeter assumption that users or devices inside the internal network should automatically be trusted. Access decisions should consider identity, device posture, location, sensitivity of the resource, session risk, and ongoing behavior. MFA is commonly used in Zero Trust, but option C is too narrow because Zero Trust applies beyond remote access and beyond MFA alone. Role-based limitations and periodic reviews are useful, but option D does not capture continuous verification. Option A is the opposite of Zero Trust because it assumes internal trust after initial authentication.

NEW QUESTION: 354
Which of the following hardening techniques must be applied on a container image before deploying it to a production environment? (Select two).
A. Remove default applications.
B. Install a NIPS.
C. Disable Telnet.
D. Reconfigure the DNS
E. Add an SFTP server.
F. Delete the public certificate.
Answer: (SHOW ANSWER)
Container image hardening best practices include removing default or unnecessary applications (A) to reduce the attack surface and disabling insecure

protocols like Telnet (C) to prevent exploitation. Minimizing software components reduces vulnerabilities and limits potential exploits.
Installing a Network Intrusion Prevention System (NIPS) (B) is a network security measure, not typically embedded in a container image. Reconfiguring DNS (D), adding an SFTP server (E), or deleting public certificates (F) are unrelated or could disrupt container functionality.
These practices are part of securing containerized environments covered under Security Architecture topics in SY0-701#6:Chapter 10 CompTIA Security + Study Guide#.

NEW QUESTION: 355
In an effort to reduce costs, a company is implementing a strategy that gives employees access to internal company resources, including email, from personal devices. Which of the following strategies is the company implementing?
A. CYOD
B. BYOD
C. COPE
D. MDM
Answer: (SHOW ANSWER)
BYOD, or Bring Your Own Device, is the correct answer because the company is allowing employees to use personally owned devices to access internal company resources such as email. In Security+ architecture and operations topics, mobile deployment models are important because each model shifts ownership, management, and risk differently. BYOD reduces hardware procurement costs, but it increases security concerns because the organization does not fully own or control the endpoint. Controls such as MDM, conditional access, encryption, remote wipe, acceptable use policies, and device compliance checks are commonly needed. CYOD means employees choose from approved corporate devices, while COPE means the company owns the device and permits personal use. MDM is a management control, not the deployment strategy itself.

NEW QUESTION: 356
An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?
A. Agent-based
B. Centralized proxy
C. URL scanning
D. Content categorization
Answer: (SHOW ANSWER)
The correct answer is A. Agent-based.
Agent-based web filtering uses software installed directly on the endpoint. Because the filtering agent runs on the laptop, it can enforce web filtering policies whether the employee is inside the office or working remotely. This avoids the need to configure additional access back to the corporate network, such as forcing all remote web traffic through an internal proxy or VPN.
Why the other options are incorrect:
B . Centralized proxy
A centralized proxy can provide web filtering, but remote users would typically need to route traffic through the corporate network or proxy service. The question specifically says the organization does not want to configure additional network access.
C . URL scanning
URL scanning checks URLs for malicious or suspicious content, but it is a filtering technique rather than the best deployment type for enforcing web filtering on laptops both inside and outside the office.
D . Content categorization

Content categorization classifies websites by type, such as gambling, social media, malware, or adult content. However, it does not describe how filtering is enforced for laptops both on and off the corporate network.
Therefore, the best answer is agent-based web filtering.

NEW QUESTION: 357
An organization needs to monitor its users' activities to prevent insider threats. Which of the following solutions would help the organization achieve this goal?
A. Behavioral analytics
B. Access control lists
C. Identity and access management
D. Network intrusion detection system
Answer: (SHOW ANSWER)
Detailed Behavioral analytics tools monitor user actions and detect anomalies that may indicate insider threats, such as unauthorized access or unusual data exfiltration activities. These tools establish baselines for normal behavior and flag deviations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Behavioral Analytics and Monitoring".

NEW QUESTION: 358
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: (SHOW ANSWER)
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: 359
A company deploys a new server that a client must be able to access it at all times. Which of the following will support this availability requirement?
A. Proxy server
B. Jump server
C. Geographic restrictions
D. Load balancer
Answer: (SHOW ANSWER)
A load balancer best supports the availability requirement because it distributes client traffic across available backend resources and can route traffic away from failed or overloaded systems. When properly implemented with multiple servers or redundant service instances, load balancing improves uptime, resilience, and service continuity. A proxy server forwards requests and may provide filtering or caching, but it does not inherently guarantee application availability. A jump server provides controlled administrative access to internal systems, not client-facing service continuity. Geographic restrictions limit access based on location and may actually reduce availability for some users. Security+ places load balancing under resilient architecture

because it helps maintain access when individual systems fail or become saturated.

NEW QUESTION: 360

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

Freecram.net

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

NEW QUESTION: 361
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: (SHOW ANSWER)
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.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 362

The Chief Information Security Officer wants to discuss options for a disaster recovery site that allows the business to resume operations as quickly as possible. Which of the following solutions meets this requirement?

A. Hot site

B. Cold site

C. Geographic dispersion

D. Warm site

Answer: (SHOW ANSWER)

NEW QUESTION: 363

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 control

B. Version changes

C. Version updates

D. Version validation

Answer: (SHOW ANSWER)

NEW QUESTION: 364

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

A. Virtualization

B. Isolation

C. Segmentation

D. Redundancy

Answer: (SHOW ANSWER)

NEW QUESTION: 365

An administrator has configured a quarantine subnet for all guest devices that connect to the network. Which of the following would be best for the security team to configure on the MDM before allowing access to corporate resources?

A. Device fingerprinting

B. Compliance attestation

C. NAC

D. 802.1X

Answer: (SHOW ANSWER)

Compliance attestation (B)ensures that devices meetpredefined security policies(e.g., encryption enabled, updated antivirus, latest OS patches) before being allowed access to corporate resources. This is commonly enforced usingMobile Device Management (MDM)systems.

By using compliance checks via MDM, only secure,policy-compliantdevices are promoted from quarantine to trusted network segments.

NEW QUESTION: 366

Which of the following would be the most appropriate way to protect data in transit?

A. SSL 3.0

B. TLS 1.3

C. SHA-256
D. AES-256
Answer: (SHOW ANSWER)

NEW QUESTION: 367
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.

NEW QUESTION: 368
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: (SHOW ANSWER)
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: 369
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: (SHOW ANSWER)
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: 370
Which of the following is a benefit of an RTO when conducting a business impact analysis?
A. It determines the likelihood of an incident and its cost.
B. It determines the roles and responsibilities for incident responders.
C. It determines the state that systems should be restored to following an incident.
D. It determines how long an organization can tolerate downtime after an incident.
Answer: (SHOW ANSWER)
Recovery Time Objective (RTO)defines themaximum acceptable downtimebefore business operations must be restored. It helps organizations set expectations for recovery speed and prioritize system restoration accordingly.
* A (likelihood of an incident and cost)relates to risk assessment, not RTO.
* B (roles and responsibilities)falls underincident response planning, not RTO.
* C (state of restored systems)is covered byRecovery Point Objective (RPO), not RTO.

NEW QUESTION: 371
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: (SHOW ANSWER)
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.

NEW QUESTION: 372
A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?
A. Business email
B. Social engineering
C. Unsecured network
D. Default credentials
Answer: (SHOW ANSWER)
The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.
* Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.
* Unsecured network is unrelated to the email content.
* Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

NEW QUESTION: 373
Which of the following is the best way to secure an on-site data center against intrusion from an insider?
A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance
Answer: (SHOW ANSWER)

NEW QUESTION: 374
In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective. Which of the following best describes the security engineer's response?
A. Risk tolerance
B. Risk acceptance

C. Risk importance
D. Risk appetite
Answer: (SHOW ANSWER)
Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

NEW QUESTION: 375
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: (SHOW ANSWER)
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: 376
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: (SHOW ANSWER)
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. Reference = 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.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 377
Which of the following activities should be included as part of passive reconnaissance in a penetration test?
A. Domain Name System (DNS) zone transfer
B. Vulnerability scanning
C. Social engineering
D. Google hacking
Answer: (SHOW ANSWER)
Google hacking is the correct passive reconnaissance activity. Passive reconnaissance collects information without directly interacting with the target's systems in a way that is likely to trigger alerts. Google hacking uses search engines and advanced search operators to discover publicly indexed information, such as exposed documents, login pages, metadata, directories, or sensitive files. DNS zone transfers require querying the target's DNS infrastructure and are considered active reconnaissance. Vulnerability scanning sends probes to target systems and is also active. Social engineering interacts with people and attempts to manipulate them, so it is not passive technical reconnaissance. In a penetration test, Google hacking is a classic OSINT method because it gathers public information without touching the target network directly.

NEW QUESTION: 378
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: (SHOW ANSWER)
"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:
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: 379
An attacker forces an internal company employee to inject malware into corporate systems under threat of publishing the employee's sensitive personal files. Which of the following best describes the attacker's motivation in this type of attack?
A. Financial gain
B. Revenge
C. Blackmail
D. Espionage
Answer: (SHOW ANSWER)
Blackmail is the correct motivation because the attacker is coercing the employee by threatening to release sensitive personal files. The attacker is not simply seeking money directly, so financial gain is not the best description. Revenge would involve retaliation for a perceived grievance, but the scenario describes coercion. Espionage involves stealing information for political, corporate, or strategic advantage, which is not the primary driver here. This is a social engineering and insider-risk scenario because an external attacker pressures an internal employee into performing malicious activity. Security+ expects candidates to recognize attacker motivations such as financial gain, ideology, espionage, revenge, and blackmail based on the pressure or incentive being used.

NEW QUESTION: 380
The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced faded log-In attempts when authenticating from the same IP address:

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

Which of the following most likely describes attack that took place?
A. Spraying
B. Brute-force
C. Dictionary
D. Rainbow table
Answer: (SHOW ANSWER)
Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

NEW QUESTION: 381
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. Sanctions
C. Fines
D. Contractual impacts

Answer: (SHOW ANSWER)

NEW QUESTION: 382
A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?
A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement
Answer: (SHOW ANSWER)
End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 29 1

NEW QUESTION: 383
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: 384
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: (SHOW ANSWER)

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: 385
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: (SHOW ANSWER)
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.
Reference = 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: 386
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 firewallsunder Domain 1.4: Security controls.

NEW QUESTION: 387
Which of the following is a primary security concern for a company setting up a BYOD program?
A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking
Answer: (SHOW ANSWER)
Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption. Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

NEW QUESTION: 388
A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?
A. MDM
B. Containerization
C. DLP
D. FIM
Answer: (SHOW ANSWER)
Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.
Containerizationisolates work applications from personal applications but does not enforce app restrictions.
Data Loss Prevention (DLP)focuses on preventing sensitive data leaks rather than managing app installations.
Therefore,MDMis the best solution for restricting unauthorized applications on personal devices.
File Integrity Monitoring (FIM)tracks changes to files and system configurations but does not control app installations.

NEW QUESTION: 389
A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?
A. Memory injection
B. Race condition
C. Side loading
D. SQL injection
Answer: (SHOW ANSWER)

Memory injection vulnerabilities allow unauthorized code or commands to be executed within a software program, leading to abnormal behavior such as generating outbound traffic over random high ports. This issue often arises from software not properly validating or encoding input, which can be exploited by attackers to inject malicious code.Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 390

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?

Pdfexam.net

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: 391
Which of the following is an example of a false negative vulnerability detection in a scan report?
A. A vulnerability that does not actually exist
B. A vulnerability that has already been remediated
C. A result that shows no known vulnerability
D. A zero-day vulnerability with a known remediation
Answer: (SHOW ANSWER)
A false negative occurs when a security control or scanning tool fails to detect a vulnerability that actually exists. In vulnerability scanning, this means the scan reports a system as secure even though it is vulnerable. Therefore, a result that shows no known vulnerability is an example of a false negative if a vulnerability is present but undetected.
CompTIA Security+ SY0-701 explains that false negatives are particularly dangerous because they provide a false sense of security, potentially leaving systems exposed to exploitation. Causes of false negatives include outdated vulnerability signatures, misconfigured scanners, credentialed scan failures, or unsupported legacy systems.
Option A describes a false positive, where a vulnerability is reported but does not exist. Option B may indicate an outdated scan result, not necessarily a false negative. Option D is incorrect because zero-day vulnerabilities do not have known remediations and are typically not detected by signature-based scanners.
Thus, the correct example of a false negative is C: A result that shows no known vulnerability.

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 392
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: (SHOW ANSWER)
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: 393
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. Reference: 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: 394
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: (SHOW ANSWER)
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. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

NEW QUESTION: 395
Which of the following tasks is typically included in the BIA process?
A. Developing the incident response plan
B. Estimating the recovery time of systems
C. Identifying the communication strategy
D. Evaluating the risk management plan
E. Establishing the backup and recovery procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 396
Which of the following should a systems administrator use to decrease the company's hardware attack surface?
A. Replication
B. Isolation
C. Centralization
D. Virtualization
Answer: (SHOW ANSWER)
Virtualization (D)allows multiple systems and services to be hosted onfewer physical machines, thereby reducing the total number of physical devicesand consequently thehardware attack surface. This also allows for better patching, monitoring, and control.
The fewer devices you manage physically, the fewer entry points there are for attackers to exploit hardware- level vulnerabilities.
NEW QUESTION: 397
A program manager wants to ensure contract employees can only use the company's computers Monday through Friday from 9 a.m. to 5 p.m. Which of the following would best enforce this access control?
A. Creating a GPO for all contract employees and setting time-of-day log-in restrictions
B. Creating a discretionary access policy and setting rule-based access for contract employees
C. Implementing an OAuth server and then setting least privilege for contract employees
D. Implementing SAML with federation to the contract employees' authentication server
Answer: (SHOW ANSWER)
The most appropriate method is to use aGroup Policy Object (GPO) with time-of-day restrictions (A). This is a native capability in Windows environments that allows administrators to controlwhen users are allowed to log into domain-joined systems.
This aligns withDomain 3.1: Given a scenario, apply identity and access management (IAM) concepts, especially under"Access controls (e.g., time-based restrictions, GPOs, least privilege)."

NEW QUESTION: 398
Which of the following best describes the purpose of using deception technologies in a security strategy?
A. To prevent malware installation through endpoint protection tools
B. To block all external traffic before it reaches critical information systems
C. To lure attackers to controlled environments to collect threat intelligence
D. To detect insider threats by monitoring privileged user accounts
Answer: (SHOW ANSWER)
Deception technologies are designed to attract, observe, and study attackers in controlled environments. Examples include honeypots, honeyfiles, honeytokens, decoy credentials, and fake services. Their value is not mainly prevention; it is detection, delay, intelligence gathering, and attacker behavior analysis. By interacting with decoys, attackers reveal tactics, techniques, procedures, tooling, source infrastructure, and objectives without reaching real production assets. Endpoint protection prevents malware execution, which is not the primary role of deception. Blocking all external traffic is a firewall or segmentation function. Privileged-user monitoring may detect insider threats, but it is not the core purpose of deception technology. Security+ treats deception as an operational detection and threat intelligence capability.

NEW QUESTION: 399
Which of the following is a directive managerial control?
A. Acceptable use policy
B. Login warning banner
C. Master service agreement
D. No trespassing sign
Answer: (SHOW ANSWER)
A directive managerial control provides guidance and expectations for behavior through policy and governance. An Acceptable Use Policy (AUP) is a classic example, as it defines how users may and may not use organizational systems and data. Security+ SY0-701 categorizes policies as managerial (administrative) controls that direct user behavior and establish accountability.
A login warning banner (B) is typically a deterrent/administrative control but is not managerial in nature. A master service agreement (C) is a contractual/legal document, not a managerial directive for internal users. A "No trespassing" sign (D) is a physical deterrent control.
Because an AUP formally directs behavior and is enforced through management processes, A: Acceptable use policy is correct.
NEW QUESTION: 400
A software development manager wants to ensure the authenticity of the code created by the company.
Which of the following options is the most appropriate?
Freecram.net
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. Reference = 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: 401
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: (SHOW ANSWER)
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: 402
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.
Reference:
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: 403
Which of the following should a security team do first before a new web server goes live?
A. Create WAF rules.
B. Apply patch management

C. Enable network intrusion detection.
D. Harden the virtual host.
Answer: (SHOW ANSWER)

NEW QUESTION: 404
An office wants to install a Wi-Fi network. The security team must ensure a secure design. The access points will be more powerful and use WPA3 with a 16-character randomized key. Which of the following should the security team do next?
A. Create a heat map of the building perimeter.
B. Deploy IPSec tunnels from each access point to the controller.
C. Enable WPA2-PSK with a 24-character randomized key.
D. Disable SSH administration on all access points.
Answer: (SHOW ANSWER)
Because the organization plans to deploy high-powered wireless access points, the next critical step is to create a heat map of the building perimeter. CompTIA Security+ SY0-701 highlights wireless heat maps as an essential design tool for identifying signal bleed, coverage overlap, dead zones, and areas where wireless signals extend beyond intended boundaries.
Stronger access points increase the risk of signal leakage outside the building, which could allow unauthorized users to attempt connections from parking lots or nearby buildings. A heat map enables the security team to visualize RF propagation and adjust power levels, antenna placement, and access point locations to minimize external exposure while maintaining internal coverage.
Deploying IPSec tunnels (B) is unnecessary for standard WLAN architectures. Enabling WPA2-PSK (C) weakens security compared to WPA3. Disabling SSH administration (D) is a hardening step but does not address wireless coverage risks.
Therefore, the correct next step in secure Wi-Fi design is A: Create a heat map of the building perimeter.

NEW QUESTION: 405
A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?
A. Jump server
B. RADIUS
C. HSM
D. Load balancer
Answer: (SHOW ANSWER)
A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host12.
RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access34.
HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them5 .
A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them .

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

NEW QUESTION: 406
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. Proxy server
B. Jump server
C. Load balancer
D. SD-WAN
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 407
Which of the following is a preventive physical security control?
A. Alarm system
B. Motion sensors
C. Video surveillance system
D. Bollards
Answer: (SHOW ANSWER)

Valid SY0-701 Dumps shared by ExamDiscuss.com for Helping Passing SY0-701 Exam! ExamDiscuss.com now offer the **newest SY0-701 exam dumps**, the ExamDiscuss.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com SY0-701 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/SY0-701/premium/ (**916** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)