DUMPSBOSS.

CompTIA SecurityX Certification Exam

CompTIA CAS-005

Version Demo

Total Demo Questions: 48

Total Premium Questions: 488

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Governance, Risk, and Compliance	76
Topic 2, Security Architecture	130
Topic 3, Security Engineering	133
Topic 4, Security Operations	149
Total	488

QUESTION NO: 1

Which of the following are the best ways to mitigate the threats that are the highest priority? (Select two).

A. Isolate network systems using Zero Trust architecture with microsegmentation and SD-WAN

B. Scan all systems and source code with access to sensitive data for vulnerabilities.

C. Implement a cloud access security broker and place it in blocking mode to prevent information exfiltration.

D. Apply data labeling to all sensitive information within the environment with special attention to payroll information.

E. Institute a technical approval process that requires multiple parties to sign off on mass payroll changes.

ANSWER: A E

Explanation:

Isolate network systems using Zero Trust architecture with microsegmentation and SD-WAN is correct because it directly reduces the impact of high-priority enterprise threats such as lateral movement, unauthorized access between trust zones, and compromise propagation. Zero Trust assumes no implicit trust based on network location and enforces continuous verification, least privilege, and tightly scoped access paths. Microsegmentation supports this by limiting east-west traffic so that a compromised system cannot freely reach sensitive systems. NIST describes Zero Trust as a model focused on protecting resources through dynamic, per-session access decisions rather than broad network trust; see NIST SP 800-207. Institute a technical approval process that requires multiple parties to sign off on mass payroll changes is also correct because it applies separation of duties and dual authorization to a high-risk business process. Payroll changes can directly create financial loss, fraud, and integrity issues, so requiring multiple independent approvals materially lowers the chance that one compromised account, insider, or process error can trigger a large unauthorized change. This aligns with security control principles such as separation of duties in NIST SP 800-53.

QUESTION NO: 2

Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem.

Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

A. Compile a list of firewall requests and compare than against interesting cloud services.

B. Implement a CASB solution and track cloud service use cases for greater visibility.

C. Implement a user-behavior system to associate user events and cloud service creation events.

D. Capture all log and feed then to a SIEM and then for cloud service events

ANSWER: B

Explanation:

Implement a CASB solution and track cloud service use cases for greater visibility is correct because a cloud access security broker is specifically designed to discover, monitor, and govern cloud service usage, including unsanctioned or unmanaged cloud services commonly described as shadow IT. In this scenario, the security team lacks visibility into who is creating cloud storage services and instances, and the pace of activity exceeds what a small team can manually review. A CASB can centralize visibility across cloud applications and services, correlate usage to users and identities, and apply policy-based controls with relatively low ongoing administrative effort compared with manual reviews or custom event correlation. CASBs commonly provide discovery, activity monitoring, risk scoring, data protection, and policy enforcement across SaaS and other cloud environments, making them well aligned to the stated need for visibility into cloud service use. This maps directly to recognized CASB functions described by Microsoft as visibility, data security, threat protection, and compliance capabilities for cloud apps, and by NIST as a brokered control point for cloud service visibility and policy enforcement. See Microsoft Defender for Cloud Apps overview and NIST CASB glossary.

QUESTION NO: 3

A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.

Based on this agreement, this finding is BEST categorized as a:

A. true positive.

B. true negative.

C. false positive.

D. false negative.

ANSWER: C

Explanation:

false positive is correct because the scanner's alert is based on the application's upstream version appearing obsolete, not on the actual security state of the package as maintained by the Linux vendor. Enterprise Linux vendors commonly backport security fixes: they keep an older, stable software version for compatibility while applying selected security patches from newer releases. As a result, simple version-based detection can report a component as vulnerable even though the vendor-supported package has already received the relevant fixes. In this scenario, the company has confirmation that the vendor has applied fixes for all current vulnerabilities and will continue supporting the software, so the detected "obsolete version" does not represent an active vulnerability under the organization's supported configuration. This is exactly the type of condition that should be documented as a false positive, typically with evidence such as vendor advisories, package changelogs, or support agreements. Red Hat describes this backporting model in its security update guidance at Red Hat Backporting Security Fixes, and NIST discusses vulnerability validation and remediation tracking practices in NIST SP 800-40 Rev. 4.

QUESTION NO: 4

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Inform users regarding what data is stored.

B. Provide opt-in/out for marketing messages.

C. Provide data deletion capabilities.

D. Provide optional data encryption.

E. Grant data access to third parties.

F. Provide alternative authentication techniques.

ANSWER: A C

Explanation:

Inform users regarding what data is stored and Provide data deletion capabilities are correct because GDPR is built around transparency and enforceable data subject rights. When an organization collects or processes personal data, it must tell individuals what personal data is being collected, why it is being processed, how long it will be retained, and who may receive it. This aligns with GDPR transparency obligations and the right to be informed, which are core requirements for any service handling personal data from individuals in the EU. A global service must therefore include clear privacy notices and mechanisms that let users understand how their information is used.

Provide data deletion capabilities is also required because GDPR gives individuals the right to erasure, commonly called the "right to be forgotten." When the legal conditions apply, users must be able to request deletion of their personal data, and the

organization must have processes to honor those requests within required timelines. These controls are practical compliance measures for a globally deployed service that may process EU personal data. See the European Commission's summary of individual GDPR rights at European Commission: My rights under GDPR and the GDPR right to erasure text at GDPR Article 17.

QUESTION NO: 5

A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.

B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.

C. The system administrator should evaluate dependencies and perform upgrade as necessary.

D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

ANSWER: C

Explanation:

The system administrator should evaluate dependencies and perform upgrade as necessary is the most appropriate corrective action because a vulnerability scan finding on an internal host typically identifies a vulnerable installed service, package, library, or platform component. The right corrective-action plan should assign remediation to the team that owns system maintenance and patching, and it should account for dependency impact before applying an upgrade. In enterprise environments, upgrading a vulnerable component without checking dependencies can break applications, middleware, agents, or integrations, so the corrective action should include evaluation, testing, and then deployment of the required update through normal change-control processes. This aligns with standard vulnerability management practices: validate the finding, determine affected assets and software dependencies, prioritize based on risk, and remediate by applying vendor-supported patches or upgrades. NIST guidance on enterprise patch management emphasizes identifying applicable updates, testing where appropriate, and deploying patches to reduce exploitable weaknesses; see NIST SP 800-40 Rev. 4. CISA also frames remediation of known software vulnerabilities around timely vendor updates and mitigation tracking; see CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 6

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. Dark web monitoring

B. Adversary emulation engagement

C. Supply chain risk consultation

D. Tabletop exercises

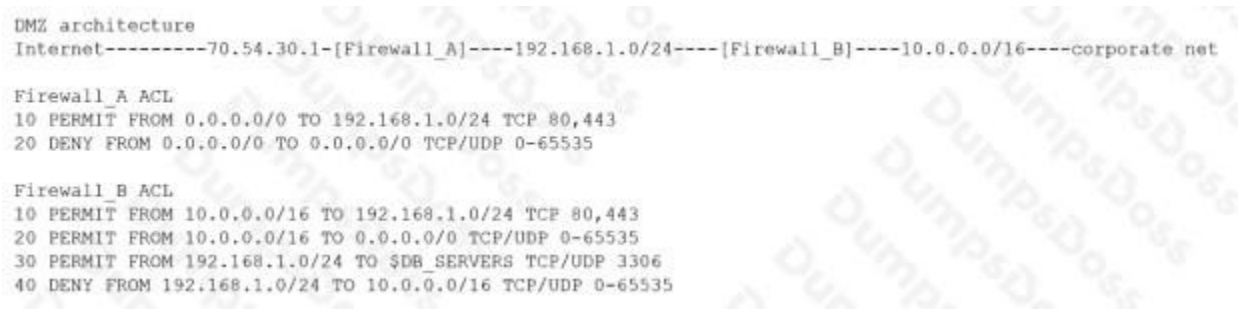
ANSWER: B

Explanation:

Adversary emulation engagement is correct because the board is not merely asking to discuss the threat; it wants to validate whether existing awareness training, technical controls, and governance will actually withstand a realistic attack scenario. An adversary emulation engagement is designed to mimic the tactics, techniques, and procedures of a real threat actor in a controlled manner. In this case, the engagement could safely simulate coordinated distraction techniques, attempts to access payment terminals, and attempts to bypass monitoring or physical security controls, while measuring how employees, processes, and technical defenses respond. This provides evidence-based assurance about control effectiveness and helps identify gaps before criminals exploit them. The approach aligns with recognized security assessment practices described by NIST SP 800-115, which covers technical security testing and examination methods, and with adversary emulation concepts documented by MITRE ATT&CK. Because the scenario is based on a specific observed threat pattern from an ISAC report, a realistic emulation is the strongest fit for testing readiness against that threat.

QUESTION NO: 7

A security architect is reviewing the following proposed corporate firewall architecture and configuration:



```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

Web servers must receive all updates via HTTP/S from the corporate network.

Web servers should not initiate communication with the Internet.

Web servers should only connect to preapproved corporate database servers.

Employees' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443

C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535

F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

ANSWER: A F

Explanation:

The most secure recommendation is to allow only the explicitly required flows using least privilege. "Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443" satisfies the employee requirement by limiting corporate user devices to outbound web services on HTTP and HTTPS only. Because the firewalls are stateful, return traffic for those approved sessions is handled without opening broad inbound access. "Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

” is also appropriate because it restricts the web-server network to a specific preapproved internal corporate host using only the required HTTP/S service ports, supporting tightly controlled update or application connectivity without allowing the web servers to initiate arbitrary Internet or internal communications. This aligns with firewall rule design best practices: define rules as narrowly as possible by source, destination, protocol, and port, and rely on stateful inspection rather than broad reciprocal permits. NIST’s firewall guidance emphasizes using restrictive rule sets and explicit traffic control between security zones: NIST SP 800-41 Rev. 1. CISA also promotes least-privilege access control as a core security practice: CISA Zero Trust Maturity Model.

QUESTION NO: 8

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 C

Explanation:

Threat feed API and Scheduled task are the correct choices because the mail server needs both a trusted source of current indicators and an automated way to refresh those indicators. A threat feed API provides machine-readable threat intelligence, such as malicious sender domains, IP addresses, URLs, file hashes, and other indicators of compromise that can be used to update filtering or block rules. This aligns with standard threat intelligence sharing practices, where organizations consume external indicator data to improve detection and prevention controls; see NIST SP 800-150 and CISA Automated Indicator Sharing. A scheduled task is also needed because the server or an associated script must periodically retrieve the latest IoCs, validate or normalize them, and apply them to the mail filtering configuration. Together, the threat feed API supplies the intelligence, and the scheduled task keeps the mail server’s local blocking list current without relying on manual updates. This combination supports proactive blocking of known-malicious incoming email based on continuously refreshed threat data.

QUESTION NO: 9

A security engineer needs to remediate a SWEET32 vulnerability in an OpenSSH-based application and review existing configurations. Which of the following should the security engineer do? (Select two.)

A. Disable Twofish algorithms

B. cat /etc/ashd/ash_config | grep "HMAC"

C. Disable RSA algorithms

D. cat /etc/sshd/ssh_config | grep "PermitRootLogin"

E. Disable 3DES algorithms

F. cat /etc/sshd/ssh_config | grep "Ciphers"

ANSWER: E F

Explanation:

Disable 3DES algorithms is correct because SWEET32 targets legacy 64-bit block ciphers, most notably Triple DES, by exploiting birthday-bound collisions after large volumes of encrypted traffic. In an SSH context, remediation means ensuring that 3DES-based cipher suites such as 3des-cbc are not allowed and that modern ciphers with larger block sizes or AEAD modes are used instead. The command cat /etc/sshd/ssh_config | grep "Ciphers" is also correct because reviewing the OpenSSH Ciphers directive is the relevant configuration check for determining which symmetric encryption algorithms are currently permitted. OpenSSH documents the Ciphers directive as the control used to specify allowed encryption algorithms, and it also identifies legacy algorithms such as 3des-cbc as older compatibility options rather than preferred modern choices. For more detail, see the OpenSSH sshd_config documentation for Ciphers and the original SWEET32 attack description.

QUESTION NO: 10

A security engineer is implementing a code signing requirement for all code developed by the organization. Currently, the PKI only generates website certificates. Which of the following steps should the engineer perform first?

A. Add a new template on the internal CA with the correct attributes.

B. Generate a wildcard certificate for the internal domain.

C. Recalculate a public/private key pair for the root C

D. Implement a SAN for all internal web applications.

ANSWER: A

Explanation:

Add a new template on the internal CA with the correct attributes is the correct first step because code signing certificates require a certificate profile that is different from a standard website/TLS certificate. In an enterprise PKI, certificate templates define the intended purpose, key usage, extended key usage, enrollment permissions, subject handling, validity period, and issuance requirements for certificates. Since the organization's PKI currently issues only website certificates, the engineer must first create or duplicate an appropriate certificate template that includes the Code Signing extended key usage and the proper security/enrollment settings for authorized developers or build systems. Once that template exists and is published by the internal CA, eligible requesters can enroll for certificates that are technically valid for signing software, scripts, or binaries. This aligns with how Microsoft AD CS certificate templates are used to control certificate purpose and issuance behavior, as described in Microsoft certificate template concepts. Code signing also depends on certificates being issued for the intended code-signing purpose, as reflected in Microsoft's guidance on cryptography and signing tools.

QUESTION NO: 11

The material finding 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? (Select two).

Setting different access controls defined by business area

A. Implementing a role-based access policy

B. Designing a least-needed privilege policy

C. Establishing a mandatory vacation policy

D. Performing periodic access reviews

E. Requiring periodic job rotation

ANSWER: A D

Explanation:

Implementing a role-based access policy and performing periodic access reviews are the best ways to mitigate privilege creep caused by employees changing roles or departments. Implementing a role-based access policy aligns permissions to

defined job functions, business responsibilities, and authorization requirements rather than assigning access individually and leaving it in place indefinitely. When users move to a new role, their access can be reassigned based on the new role profile, which supports least privilege and reduces the chance that old departmental permissions remain attached to the account.

Performing periodic access reviews is equally important because privilege creep is often discovered only after permissions accumulate over time. Regular reviews allow managers, system owners, and security teams to validate whether each user still has a legitimate business need for assigned access. This is a common identity governance and access management control used to detect excessive permissions, remove stale entitlements, and support audit readiness. NIST describes access control reviews and role-based access control as key mechanisms for managing authorization and enforcing least privilege; see NIST Role Based Access Control and NIST SP 800-53 Rev. 5.

QUESTION NO: 12

A company isolated its OT systems from other areas of the corporate network These systems are required to report usage information over the internet to the vendor Which oi the following b*st reduces the risk of compromise or sabotage ' (Select two).

A. Implementing allow lists

B. Monitoring network behavior

C. Encrypting data at rest

D. Performing boot integrity checks

E. Executing daily health checks

F. Implementing a site-to-site IPSec VPN

ANSWER: A F

Explanation:

Implementing allow lists and implementing a site-to-site IPSec VPN are the best choices because they directly reduce the exposure created when isolated OT systems must communicate externally. Implementing allow lists limits outbound and inbound communication to explicitly approved destinations, ports, protocols, applications, or services. In an OT environment, this is especially valuable because systems are often purpose-built and predictable, making strict allow-listing a practical way to reduce unauthorized access paths and limit opportunities for malicious commands or unexpected traffic. Implementing a site-to-site IPSec VPN adds authenticated, encrypted connectivity between the OT environment and the vendor, helping ensure that usage data is sent through a protected tunnel rather than exposed directly across the internet. Together, these controls preserve the benefits of segmentation while enabling required vendor reporting through tightly controlled and secured communications. This aligns with common industrial control system guidance that emphasizes network segmentation, controlled external connectivity, and secure remote communications for OT environments. See CISA ICS Recommended Practices and NIST SP 800-82 Rev. 3.

QUESTION NO: 13

During a recent security event, access from the non-production environment to the production environment enabled unauthorized users to install unapproved software and make unplanned configuration changes. During an investigation, the following findings are identified:

• Several new users were added in bulk by the IAM team.

• Additional firewalls and routers were recently added to the network.

• Vulnerability assessments have been disabled for all devices for more than 30 days.

• The application allow list has not been modified in more than two weeks.

• Logs were unavailable for various types of traffic.

• Endpoints have not been patched in more than ten days.

Which of the following actions would most likely need to be taken to ensure proper monitoring is in place within the organization? (Select two)

A. Disable bulk user creations by the IAM team.

B. Extend log retention for all security and network devices for 180 days for all traffic.

C. Review the application allow list on a daily basis to make sure it is properly configured.

D. Routinely update all endpoints and network devices as soon as new patches/hot fixes are available.

E. Ensure all network and security devices are sending relevant data to the SIEM.

F. Configure rules on all firewalls to only allow traffic from the production environment to the non-production environment.

ANSWER: B E

Explanation:

Extend log retention for all security and network devices for 180 days for all traffic and Ensure all network and security devices are sending relevant data to the SIEM are the best actions because the central issue is inadequate monitoring and visibility. If logs are unavailable for various traffic types, security teams cannot reliably detect unauthorized access, correlate activity across environments, or reconstruct what happened during an investigation. Longer retention gives analysts enough historical data to identify slow-moving attacks, compare current behavior with prior baselines, and support compliance or forensic requirements. Sending relevant telemetry from firewalls, routers, and security devices into the SIEM is equally important because newly added infrastructure can create blind spots if it is not onboarded into centralized monitoring. A SIEM depends on complete, timely log ingestion to correlate events, alert on suspicious activity, and provide an organization-wide operational picture. This aligns with log management and continuous monitoring guidance, including NIST's recommendations for collecting, retaining, reviewing, and analyzing security event data in NIST SP 800-92 and ongoing monitoring concepts in NIST SP 800-137.

QUESTION NO: 14

An organization is developing an in-house software platform to support capital planning and reporting functions. In addition to role-based access controls and auditing/logging capabilities, the product manager must include requirements associated with archiving data and immutable backups. Which of the following organizational considerations are most likely associated with this requirement? (Select two)

A. Crypto-export management controls

B. Supply chain weaknesses

C. Device attestation

D. Quality assurance

E. Legal hold compliance

F. Ransomware resilience

ANSWER: E F

Explanation:

Legal hold compliance and Ransomware resilience are the correct organizational considerations because archiving and immutable backups are primarily about preserving data integrity, availability, and evidentiary value over time. Legal hold compliance requires an organization to retain potentially relevant records when litigation, investigation, audit, or regulatory action is anticipated. In that context, archived data must be protected from alteration or deletion so the organization can demonstrate that records were preserved in a trustworthy state. Microsoft's eDiscovery guidance describes legal holds as a mechanism for preserving content that may be relevant to legal or compliance matters: Microsoft Purview eDiscovery legal hold.

Ransomware resilience is also directly supported by immutable backups because the organization needs recoverable copies that attackers cannot encrypt, modify, or destroy. Immutable or write-protected backups help ensure restoration is possible even if production systems and ordinary backup repositories are compromised. This aligns with CISA ransomware guidance, which recommends maintaining offline, encrypted, immutable backups as part of ransomware preparation and recovery planning: CISA StopRansomware Guide. Together, these requirements support both compliance-driven retention and operational recovery after destructive attacks.

QUESTION NO: 15 - (SIMULATION)

A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization Which of the following actions best enables the team to determine the scope of Impact?

A. Performing a port scan

B. Inspecting egress network traffic

C. Reviewing the asset inventory

D. Analyzing user behavior

ANSWER: See the explanation for the answer

Explanation:

Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.

Performing a port scan (Option A) might help identify open ports but does not provide specific information about theapplication versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected.

QUESTION 1

A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

A. Disable User2's account

B. Disable User12's account

C. Disable User8's account

Answer: D. Disable User1's account D

Based on the provided authentication logs, we observe that User1's accountexperienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Heres a breakdown of why disabling User1's account is the appropriate first step:

Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts: VM01 at 8:01:23 AM

VM08 at 8:01:23 AM VM01 at 8:01:23 AM VM08 at 8:01:23 AM

Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.

Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further

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

NIST Special Publication 800-63B: Digital Identity Guidelines

By addressing User1's account first, we effectively mitigate the immediate threat of a brute-force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

QUESTION 2

Which of the following AI concerns is most adequately addressed by input sanitation?

A. Model inversion

B. Prompt Injection

C. Data poisoning

Answer: D. Non-explainable model B

Input sanitation is a critical process in cybersecurity that involvesvalidating 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 realtime 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.

Reference:

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

QUESTION 3

A systems administrator wants to introduce a newly released feature for an internal application. The administrate docs not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?

A. Staging environment

B. Testing environment

C. CI/CO pipeline

Answer: D. Development environment A

The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Heres a detailed explanation:

Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.

Isolation fromProduction: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.

Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.

Reference:

CompTIA Security+ SY0-601 Official Study Guide by Quentin Docter, Jon Buhagiar

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

QUESTION 4

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

C. UBA rules and use cases

D. TAXII/STIX library

Answer: A

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

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.

QUESTION 5

After an incident occurred, a team reported during the lessons-learned review that the team.

* Lost important Information for further analysis.

* Did not utilize the chain of communication

* Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findinds?

A. Requestingbudget for better forensic tools to Improve technical capabilities for Incident response operations

B. Building playbooks for different scenarios and performing regular table-top exercises

C. Requiring professional incident response certifications tor each new team member

Answer: D. Publishing the incident response policy and enforcing it as part of the security awareness program B

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide" SANS Institute, "Incident Handler's Handbook"

QUESTION 6

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

Exfiltration of intellectual property Unencrypted files

Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A. Implementing data loss prevention

B. Deploying file integrity monitoring

C. Restricting access to critical file services only

D. Deployingdirectory-based group policies

E. Enabling modem authentication that supports MFA

F. Implementing a version control system

Answer: G. Implementing a CMDB platform A,E

To mitigate the identified vulnerabilities, the followingsolutions are most appropriate:

A . Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

E . Enabling modern authentication that supports Multi-Factor Authentication (MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned: B . Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords.

C . Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

D . Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

F . Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

G . Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations" CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

QUESTION 7

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

Unauthorized reading and modification of data and programs Bypassing application security mechanisms

Privilege escalation

interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

A. SELinux

B. Privileged access management

C. Self-encrypting disks

D. NIPS

Answer: A

The most appropriate solution for the systems engineer to deploy is SELinux (Security-Enhanced Linux). Here's why:

Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system

Security Mechanisms: SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.

Privilege Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl NSA's Guide to the Secure Configuration of Red Hat Enterprise Linux 5 (SELinux)

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

QUESTION 8

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=dmarc 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 CNAMErecord 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:l92.168.1.11 include my-email.com -ell"

F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"

Answer: G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server B,D

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

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

QUESTION 9

Within a SCADA a business needs access to the historian server in order together metric about the functionality of the environment. Which of the following actions should be taken to address this requirement?

A. Isolating the historian server for connections only from The SCADA environment

B. Publishing the C$ share from SCADA to the enterprise

C. Deploying a screened subnet between 11 and SCADA

Answer: D. Adding the business workstations to the SCADA domain A

The best action to address the requirement of accessing the historian server within a SCADA system is to isolate the historian server for connections only from the SCADAenvironment. Heres why: Security and Isolation: Isolating the historian server ensures that only authorized devices within the SCADA environment can connect to it. This minimizes the attack surface and protects sensitive data from unauthorized access.

Access Control: By restricting access to the historian server to only SCADA devices, the organization can better control and monitor interactions, ensuring that only legitimate queries and data retrievals occur.

Best Practices for Critical Infrastructure: Following the principle of least privilege, isolating critical components like the historian server is a standard practice in securing SCADA systems, reducing the risk of cyberattacks.

Reference:

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

NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security ISA/IEC 62443 Standards: Security for Industrial Automation and Control Systems

QUESTION 10

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

B. Sating and hashing

C. Account federation with hardware tokens

D. SAE

E. Key splitting

Answer: E

The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Heres why:

Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts anddistributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.

Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.

Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl NIST Special Publication 800-57: Recommendation for Key Management

ISO/IEC 27002:2013: Information Technology - Security Techniques - Code of Practice for Information Security Controls

By employing key splitting, organizations can effectively reduce the risk ofinsider threats and enhance the overall security of encrypted material.

QUESTION 11

A vulnerability can on a web server identified the following:

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_AE3_256_GCMS_HA256

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

Answer: F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA B,C

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:

B . 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.

C . 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.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"

OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

QUESTION 12

The identity and access management team is sending logs to the SIEM for continuous monitoring.

The deployed log collector isforwarding logs to

the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

A. The compute resources are insufficient to support the SIEM

B. The SIEM indexes are 100 large

C. The data is not being properly parsed

Answer: D. The retention policy is not property configured C

Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows

QUESTION 13

An incident response team is analyzing malware and observes the following: Does not execute in a sandbox

No network loCs

No publicly known hash match

No process injection method detected

Which of thefollowing 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

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 themalware'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

QUESTION 14

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

Answer: D. Risk appetite directly influences which breaches are disclosed publicly A

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.

Reference:

CompTIA Security+ Study Guide

NIST Risk Management Framework (RMF) guidelines ISO 31000, "Risk Management “ Guidelines"

QUESTION 15

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 thefollowing 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

Answer: D. Managing key material on a HSM D

The beststrategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Heres why:

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.

Reference:

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

ISO/IEC 19790:2012: Information Technology - Security Techniques - Security Requirements for Cryptographic Modules

QUESTION 16

Users are willing passwords on paper because of the number of passwords needed in an environment. Which of the following solutions is the best way to manage this situation and decrease risks?

A. Increasing password complexity to require 31 least 16 characters

B. implementing an SSO solution and integrating with applications

C. Requiring users to use an open-source password manager

Answer: D. Implementing an MFA solution to avoid reliance only on passwords B

Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Heres why:

Reduced Password Fatigue: SSO allows users tolog in once and gain access to multiple applications and systems without needing to remember and manage multiple passwords. This reduces the likelihood of users writing down passwords.

Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication methods.

User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.

Reference:

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

NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management

OWASP Authentication Cheat Sheet

QUESTION 17

The material finding 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? (Select two).

Setting different access controls defined by business area

A. Implementing a role-based access policy

B. Designing a least-needed privilege policy

C. Establishing a mandatory vacation policy

Answer: E. Requiring periodic job rotation A,D

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.

Reference:

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

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

Performing Periodic Access Reviews:

RegularAudits: Periodic access reviews help identify and rectify instances of privilege creep by ensuring that users' access permissions are appropriate for their current roles. These reviews can highlight unnecessary or outdated permissions, allowing for timely adjustments.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl ISO/IEC 27001:2013 - Information Security Management

QUESTION 18

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

Be survivable to one environmental catastrophe

CK recoverable within 24 hours of critical loss of availability

Be resilient to active exploitation of one site-to-site VPN solution

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. Use orchestration to procure, provision, and transfer application workloads lo cloud services

Answer: F. Implement full weekly backups to be stored off-site for each of the company's sites B

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant

Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.

Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.

Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

Reference:

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

NIST Special Publication 800-34: Contingency Planning Guide for Federal Information Systems ISO/IEC 27031:2011 - Guidelines for Information andCommunication Technology Readiness for Business Continuity

QUESTION 19

Users must accept the terms presented in a captive petal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network A network engineer observes the following:

Users should be redirected to the captive portal. The Motive portal runs Tl. S 1 2

Newer browser versions encounter security errors that cannot be bypassed Certain websites cause unexpected CK directs

Which of the following mow likely explains this behavior?

A. The TLS ciphers supported by the captive portal ate deprecated

B. Employment of the HSTS setting is proliferating rapidly.

C. Allowed traffic rules are causing the NIPS to drop legitimate traffic

Answer: D. An attacker is redirecting supplicants to an evil twin WLAN. A

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Heres why:

TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

HSTS and Browser Security: Browsers with HTTP Strict Transport Security (HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

Reference:

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

OWASP Transport LayerProtection Cheat Sheet

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

QUESTION 20

A security configure isbuilding 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

Answer: D. The /etc/etc/sshd, configure file updating the ciphers D

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.

Reference:

CompTIA Security+ Study Guide OpenSSH manual pages (man sshd_config) CIS Benchmarks for Linux

QUESTION 21

A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization Which of the following actions best enables the team to determine the scope of Impact?

A. Performing a port scan

B. Inspecting egress network traffic

C. Reviewing the asset inventory

Answer: D. Analyzing user behavior C

Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.

Performing a port scan (Option A) might help identify open ports but does not provide specific information about theapplication versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"

CIS Controls, "Control 1: Inventory and Control of Hardware Assets" and "Control 2: Inventory and Control of Software Assets"

QUESTION 22

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

Answer: D. Implementing data obfuscation B

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 ittransforms the data into a fixedlength 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

An organization is developing on AI-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the AI workload the organization wants to Implement guardrails within the platform. Which of the following should the company do to secure the AI environment?

A. Limn the platform's abilities to only non-sensitive functions

B. Enhance the training model's effectiveness.

C. Grant the system the ability to self-govern

D. Require end-useracknowledgement of organizational policies.

Answer: A

Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse.

Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations" ISO/IEC 27001, "Information Security Management"

QUESTION 24

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows:

Full disk encryption is enabled. "Always On" corporate VPN is enabled. eFuse-backed keystore is enabled.

Wi-Fi 6 is configured with SAE.

Location services is disabled.

Application allow list is unconfigured.

Assuming the hospital policy cannot be changed, which of the following is the best way to meet the hospital's objective?

B. Cryptographically erase FDE volumes

C. Issue new MFA credentials to all users

Answer: D. Configure the application allow list B

The key requirement is toinstantly eliminate data losson a lost device.

Cryptographic erasureworks by deleting encryption keys used for FDE (full disk encryption), rendering all data unrecoverable within seconds ” satisfying the "mitigate within seconds" requirement.

Revoking certificates wont wipe the data from a lost tablet.

Changing MFA credentials wont help unless the device is secured, and app allow lists dont apply post-loss.

FromCAS-005, Domain 3: Secure Systems Design and Deployment:

œCryptographic erase (CE) renders data irrecoverable by deleting encryption keys used to protect data on the device.

Reference:CAS-005 Guide, Chapter 9: Endpoint Security, pg. 178“180

QUESTION 25

A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective'

A. improving security dashboard visualization on SIEM

B. Rotating API access and authorization keys every two months

C. Implementing application toad balancing and cross-region availability

Answer: D. Creating WAF policies for relevant programming languages D

The best way to prevent application-focused attacks for a platform-as-a-service solution with a webbased front end is to create Web Application Firewall (WAF) policies for relevant programming

languages. Here's why:

Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.

Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known

Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl OWASP Top Ten: Web Application Security Risks

NIST Special Publication 800-95: Guide to Secure Web Services

QUESTION 26

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	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\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

Answer: D. A PDF that exposed sensitive information improperly B

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

QUESTION 27

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

C. Purchasing and deploying commercial off the shelf aggregation software

Answer: D. Migrating application usage logs to on-premises storage A

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.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl NIST Special Publication 800-95: Guide to Secure Web Services

OWASP API Security Top Ten

QUESTION 28

A developer needs toimprove 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

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. Here's why:

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,

Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.

Reference:

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

NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management

OWASP Password Storage Cheat Sheet

QUESTION 29

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	207
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

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencingsignificantly 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.

Reference:

CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies NIST SP 800-44, "Guidelines on Securing Public Web Servers"

QUESTION 30

A security officer received several complaints from usersabout excessive MPA 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 MI~A notifications''

A. Provisioning FID02 devices

B. Deploying a text message based on MFA

C. Enabling OTP via email

Answer: D. Configuring prompt-driven MFA D

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 specificactions 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.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-63B, "Digital Identity Guidelines"

"Multi-Factor Authentication: Best Practices" by Microsoft

QUESTION 31

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	10.123.34.90	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	10.60.65.11	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

Answer: D. Deploying a WAF with virtual patching upstream of the affected systems A

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.

A . 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.

B . Recompiling the affected programs with the most current patches: While this can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.

C . Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.

D . Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.

Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.

Reference:

CompTIA Security+ Study Guide

QUESTION 32

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

A. Incomplete mathematical primitives

B. No use cases to drive adoption

C. Quantum computers not yetcapable

Answer: D. insufficient coprocessor support D

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, providing strong privacy guarantees. However, the adoption of homomorphic encryption is challenging due to several factors:

A . Incomplete mathematical primitives: This is not the primary barrier as the theoretical foundations of homomorphic encryption are well-developed.

B . No use cases to drive adoption: There are several compelling use cases for homomorphic encryption, especially in privacy-sensitive fields like healthcare and finance.

C . Quantum computers not yet capable: Quantum computing is not directly related to the challenges of adopting homomorphic encryption.

D . Insufficient coprocessor support: The computational overhead of homomorphic encryption is significant, requiring substantial processing power. Current general-purpose processors are not optimized for the intensive computations required by homomorphic encryption, limiting its practical deployment. Specialized hardware or coprocessors designed to handle these computations more efficiently are not yet widely available.

Reference:

CompTIA Security+ Study Guide

"Homomorphic Encryption: Applications and Challenges" by Rivest et al. NIST, "Report on Post-Quantum Cryptography"

QUESTION 33

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

A. Improve firewall rules to avoid access to those platforms.

B. Implement a cloud-access security broker

Answer: D. Deploy an internet proxy that filters certain domains B

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies

as cloud-based resources are accessed. Implementing a CASB provides several benefits:

A . Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

B . Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

C . Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

D . Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.

Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services.

Reference:

CompTIA Security+ Study Guide

Gartner, "Magic Quadrant for Cloud Access Security Brokers"

NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

QUESTION 34

An organization wants to create a threat model to identity 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

Whencreating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Heres why: Exposure to Attack: External-facinginfrastructure is directly exposed to the internet, making it a

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.

Reference:

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

QUESTION 35

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

Answer: D. Non-conformance to accepted manufacturing standards C

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. Heres 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

Third partiesnotified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

A. Using IaC to include the newest dependencies

B. Creating a bug bounty program

C. Implementing a continuous security assessment program

Answer: D. Integrating a SASI tool as part of the pipeline D

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Heres why:

Early Detection: SAST tools analyze source code for vulnerabilities before the code is compiled. This allows developers to identify and fix security issues early in the development process.

Continuous Security: By integrating SAST tools into the CI/CD pipeline, the organization ensures continuous security assessment of the codebase, including third-party libraries, with each code commit and build.

Comprehensive Analysis: SAST tools provide a detailed analysis of the code, identifying potential vulnerabilities in both proprietary code and third-party dependencies, ensuring that known issues in libraries are addressed promptly.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl OWASP Static Analysis Security Testing (SAST) Cheat Sheet

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

QUESTION 37

While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

A. Spear-phishing campaign

B. Threat modeling

C. Red team assessment

Answer: D. Attack pattern analysis A

The situation where several employees were contacted by the same individual impersonating a recruiter best describes aspear-phishing campaign. Heres why:

Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.

Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spearphishing to gain the trust of the targeted individuals and increase the likelihood of a successful

attack.

Correlated Contacts: The fact that several employees were contacted by the same individual suggests a coordinated effort to breach the organizations security by targeting multiple points of entry through social engineering.

Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl NIST Special Publication 800-61: Computer Security Incident Handling Guide OWASP Phishing Cheat Sheet

QUESTION 38

During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host 0WIN23 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.

Answer: D. 0W1N29 spreads the malware through other hosts in the network A

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).

A . 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

B . LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector. C . The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.

D . OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-53, "Security and Privacy Controls forInformation Systems and Organizations" Microsoft's Windows 7 End of Support documentation

QUESTION 39

Emails that the marketing department is sending to customers are pomp to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three.)

A. DMARC

B. SPF

C. DKIM

D. DNSSEC

E. SASC

F. SAN

G. SOA

H. MX

Answer: A,B,C

To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server'scertificates:

A . DMARC (Domain-based Message Authentication, Reporting & Conformance): DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.

B . SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.

C . DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to email headers, allowing the

D . DNSSEC (Domain Name System Security Extensions): DNSSEC adds security to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam.

E . SASC: This is not a relevant standard for this scenario.

F . SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues.

G . SOA (Start of Authority): SOA records are used for DNS zone administration and do not directly impact email deliverability.

H . MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which

is handled by SPF, DKIM, and DMARC. Reference:

CompTIA Security+ Study Guide

RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC)

NIST SP 800-45, "Guidelines on Electronic Mail Security"

QUESTION 40

Users are experiencing a variety of issueswhen 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 wtiilc working remotely Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues? (Select 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.

Answer: F. Validate MDM asset compliance A,F

The reported issues suggest problems related to network connectivity, remote access, and certificate management:

A . 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.

devices might be blocked from accessing certain resources.

B . Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.

C . Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.

D . Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.

E . Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.

Reference:

CompTIA Security+ Study Guide

NIST SP800-77, "Guide to IPsec VPNs"

CIS Controls, "Control 11: Secure Configuration for Network Devices"

QUESTION 41

A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team's task'

A. Static application security testing

B. Software composition analysis

C. Runtime application self-protection

Answer: D. Web application vulnerability scanning A

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

A . Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.

B . Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.

C . Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.

D . Web application vulnerability scanning: This involves scanning the running application for

CompTIA Security+ Study Guide

OWASP (Open Web Application Security Project) guidelines on SAST NIST SP 800-95, "Guide to Secure Web Services"

Top of Form Bottom of Form

QUESTION 42

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 threatmodeling?

A. ATT&CK

B. OWASP

C. CAPEC

D. STRIDE

Answer: D

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. Heres 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.

Reference:

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

QUESTION 43

Recent repents 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:

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

Answer: D. Not allowing users to change their local passwords C

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. Heres 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

QUESTION 44

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?

B. Configuring a SASb solution to restrict users to server communication

C. Implementing microsegmentation on the server VLANs

Answer: D. installing a firewall and making it the network core C

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Heres why:

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.

Reference:

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

NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies CIS Controls: Control 12 - Boundary Defense

QUESTION 45

A security architect wants to develop abaseline 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

To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Heres 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

Reference:

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

QUESTION 46

A company updates itscloud-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 lo 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

Answer: F. Pipeline compliance scanning B,D

B . Pre-commit code linting: Linting tools analyze code for syntax errors andadherence 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.

Reference:

"Continuous Integration and Continuous Delivery" by Jez Humble and David Farley OWASP (Open Web Application Security Project) guidelines on secure coding practices

QUESTION 47

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

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 ofthreat 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 andtechniques 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.

Reference:

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"

QUESTION 48

An organization mat performs real-time financial processing is implementing a new backup solution

* 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

Answer: D. Setting up antitempering on the databases to ensure data cannot be changed unintentionally
A

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.

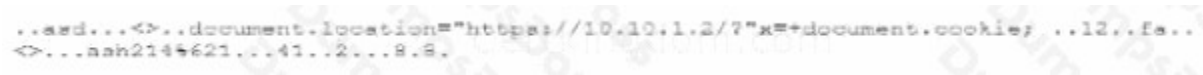
Reference:

CompTIA Security+ Study Guide

NIST SP 800-209, "Security Guidelines for Storage Infrastructure" "Immutable Backup Architecture" by Veeam

QUESTION 49

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



Which of the following best describes this incident?

B. Command injection

C. Stored XSS

Answer: D. SQL injection C

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 theuser'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.

Reference:

CompTIA Security+ Study Guide

OWASP (Open Web Application SecurityProject) guidelines on XSS

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

QUESTION 50

A security architect for a global organization with a distributed workforce recently received funding

lo deploy a CASB solution Which of the following most likely explains the choice to use a proxy-based CASB?

A. The capability to block unapproved applications and services is possible

B. Privacy compliance obligations are bypassed when using a user-based deployment.

C. Protecting and regularly rotating API secret keys requires a significant time commitment

Answer: D. Corporate devices cannot receive certificates when not connected to on-premises devices A

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block

Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.

Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.

Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.

Reference:

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

NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies Gartner CASB Market Guide

QUESTION 51

	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

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:

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

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

Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly

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.

Reference:

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

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

QUESTION 52

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

Answer: D. Enabling client device logging and system event auditing C

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. Heres 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. Reference:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl NIST Special Publication 800-92: Guide to Computer Security Log Management OWASP Logging Cheat Sheet

QUESTION 53

A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process'

B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.

C. Implement a shadow IT detection process to avoid rogue devices on the network

D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

Answer: D

To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Heres why:

Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs. Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.

Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats. Reference:

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 1 - Inventory and Control ofHardware Assets

QUESTION 54

A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

A. Improving patching processes

B. Implementing digital signature

C. Performing manual updates via USB ports

Answer: D. Allowing only dies from internal sources B

Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with amalicious version) would

A . Improving patching processes: While important, this does not directly address the issue of verifying the integrity of binaries.

B . Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.

C . Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.

D . Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-57, "Recommendation for Key Management"

OWASP (Open Web Application Security Project) guidelines on code signing

QUESTION 55

A company isolated its OT systems from other areas of the corporate network These systems are required to report usage information over the internet to the vendor Which oi the following b*st reduces the risk of compromise or sabotage' (Select two).

A. Implementing allow lists

B. Monitoring network behavior

C. Encrypting data at rest

D. Performing boot Integrity checks

E. Executing daily health checks

Answer: F. Implementing a site-to-site IPSec VPN A,F

A . Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.

F . Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception

and tampering during transit.

Other options:

B . Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.

C . Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.

D . Performing boot integrity checks: Ensures the integrity of the system at startup but does not

E . Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security" "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill

QUESTION 56

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 > /ete/passwd

B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the followingalerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical

C. Designing a muiticontainer 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

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 anattacker 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.

Reference:

CompTIA Security+ Study Guide

Docker documentation on security best practices

NIST SP 800-190, "Application Container Security Guide"

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

Answer: D. The organization has suffered brand reputation damage from incorrect media coverage C

Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.

A . The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.

B . The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence. C . The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organizations operations, especially if they involve data transfers or processing data from these countries.

D . The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.

Reference:

CompTIA Security+ Study Guide

GDPR and other global data protection regulations

"Data Sovereignty: TheFuture of Data Protection?" by Mark Burdon

QUESTION 58

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	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr011.com	GET	Blocked	Blocked	No
account2	p4yr011.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	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

Answer: D. utilizing allow lists on the WAF for all users using GFT methods C

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. Heres 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 doesnt 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. Its 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 doesnt specifically address the need for quick detection and response to internal threats.

Reference:

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

"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

QUESTION 59

A security analyst received anotification 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 m order to avoid false positives

B. Configure the scan policy to avoid targeting an out-of-scope host

C. Set network behavior analysis rules

Answer: D. Quarantine the scanner sensor to perform a forensic analysis D

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.

Heres 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

Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanners 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 scanners 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.

Reference:

CompTIA SecurityX Study Guide

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

QUESTION 60

A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

A. Third-party reports and logs

B. Trends

C. Dashboards

D. Alert failures

E. Network traffic summaries

Answer: F. Manual review processes A,B

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

A . Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential

B . Trends: Analyzing trends over time can help inunderstanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.

Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.

Reference:

CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.

NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.

"Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

QUESTION 61

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 thefollowing 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

Answer: D. Block vendor com for repeated attempts to send suspicious messages D

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. Heres the analysis of the options provided:

A . Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely

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.

QUESTION 62

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 com 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 LOAP Which of the following is me bÂ»Â« way to reduce the risk oi reoccurrence?

A. Enforcing allow lists for authorized network pons and protocols

B. Measuring and attesting to the entire boot chum

C. Rolling the cryptographic keys used for hardware security modules

Answer: D. Using code signing to verify the source of OS updates D

The scenario describes a sophisticated attack where the threat actor used steganography within LDAP

Heres 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 doesnt directly mitigate the risk of data exfiltration through network channels.

C . Rolling thecryptographic keys used for hardware security modules: This is useful for securing data and communications but doesnt 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 doesnt 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

QUESTION 63

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. Performing vulnerability tests on each device delivered by the providers

B. Performing regular red-team exercises on the vendor production line

C. Implementing a monitoring process for the integration between the application and the vendor appliance

Answer: D. Implementing a proper supply chain risk management program D

Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain. Implementing a proper supply chain risk

Vendor Management: It includes thorough vetting of suppliers and ongoing assessments of their security practices, which can identify and mitigate vulnerabilities early.

Regular Audits and Assessments: A robust SCRM program involves regular audits and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices. Collaboration and Communication: Ensures that there is effective communication and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.

Other options, while beneficial, do not provide the same comprehensive risk management:

A . Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.

B . Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.

C . Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

ISO/IEC 27036-1:2014, "Information technology ” Security techniques ” Information security for supplier relationships"

QUESTION 64

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: D

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

Reference:

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 TechnologyProfessionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

QUESTION 65

A user submits a help desk ticket stating then account does not authenticatesometimes. An analyst reviews the following logs for the user:

Which of the following best explains the reason the user's access is being denied?

A. incorrectly typed password

B. Time-based access restrictions

C. Account compromise

Answer: D. Invalid user-to-device bindings B

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

Reference:

CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

"Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

QUESTION 66

A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?

B. Scanning credentials

C. Exploit definitions

Answer: D. Testing cadence B

When differentiating between valid and invalid findings from vulnerability scans, the systemsadministrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.

Reference:

CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.

"Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.

"The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

QUESTION 67

A company that relies on an COL system must keep it operating until a new solution is available Which of the following is the most secure way to meet this goal?

A. Isolating the system and enforcing firewall rules to allow access to only required endpoints

B. Enforcing strong credentials and improving monitoring capabilities

C. Restricting system access to perform necessary maintenance by the IT team

Answer: D. Placing the system in a screened subnet and blocking access from internal resources A

To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.

Reference:

NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating critical systems and using firewalls to control access.

"Network Security Assessment" by Chris McNab: Discusses techniques for isolating systems and enforcing firewall rules to protect vulnerable or legacy systems.

By isolating the system and implementing strict firewall controls, the organization can maintain the necessary operations securely while working on deploying a new solution.

QUESTION 68

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 userinadvertently tripped the impossible travel security rule in the SSO system.

B. A threat actor has compromised the user's account and attempted to lop, m

C. The user is not allowed to access the human resources system outside of business hours

Answer: D. The user did not attempt to connect from an approved subnet A

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

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-63B, "Digital Identity Guidelines" "Impossible Travel Detection," Microsoft Documentation

QUESTION 69

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

Answer: D. Deploy a software asset manager B

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.

Reference:

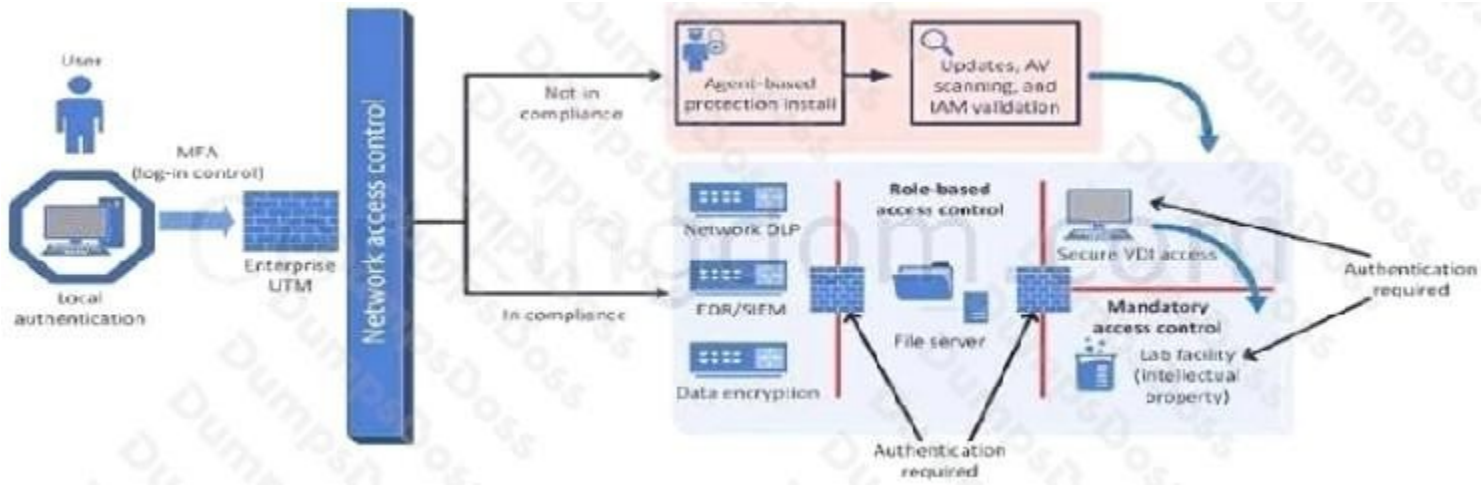
CompTIA SecurityX Study Guide

NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices

"Mobile Device Management Overview," Gartner Research

QUESTION 70

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

Answer: D. Zero Trust security model D

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is asecurity 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

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-207, "Zero Trust Architecture" "Implementing a Zero Trust Architecture," Forrester Research

QUESTION 71

A financial services organization is using Al lo fully automate the process of deciding client loan rates Which of the following should the organization be most concerned about from a privacy perspective?

A. Model explainability

B. Credential Theft

C. Possible prompt Injections

Answer: D. Exposure to social engineering A

When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.

Why Model Explainability is Critical:

Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients.

Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making fair and unbiased decisions.

Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals' financial status, can be explained and justified.

Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions are transparent and justifiable.

Other options, such ascredential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decisionmaking. Reference:

CompTIA SecurityX Study Guide

"The Importance ofExplainability in AI," IEEE Xplore

GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

QUESTION 72

A company wants to use IoT devices to manage and monitor thermostats at all facilities The thermostats must receive vendor security updates and limit access to other devices within the organization Which of the following best addresses the company's requirements"

B. Operating Iot devices on a separate network with no access to other devices internally

C. Only allowing operation for IoT devices during a specified time window

Answer: D. Configuring IoT devices to always allow automatic updates B

The best approach for managing and monitoring IoT devices, such as thermostats, is to operate them on a separate network with no access to other internal devices. This segmentation ensures that the IoT devices are isolated from the main network, reducing the risk of potential security breaches affecting other critical systems. Additionally, this setup allows for secure vendor updates without exposing the broader network to potential vulnerabilities inherent in IoT devices.

Reference:

CompTIA SecurityX Study Guide: Recommends network segmentation for IoT devices to minimize security risks.

NIST Special Publication 800-183, "Network of Things": Advises on the isolation of IoT devices to enhance security.

"Practical IoT Security" by Brian Russell and Drew Van Duren: Discusses best practices for securing IoT devices, including network segmentation.

QUESTION 73

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

Answer: D. Purchasing insurance D

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. Thismethod 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

"Information Security Risk Assessment Toolkit" by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

QUESTION 74

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).

Implementing DLP controls preventing sensitive data from leaving Company B's network

A. Documenting third-party connections used by Company B

B. Reviewing the privacy policies currently adopted by Company B

C. Requiring data sensitivity labeling tor all files shared with Company B

D. Forcing a password reset requiring more stringent passwords for users on Company B's network

Answer: E. Performing an architectural review of Company B's network A,B

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:

A . Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.

E . Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface.

These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

Reference:

CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.

NIST Special Publication 800-37, "Guide for Applying the RiskManagement Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.

"Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance ofsecurity assessments during acquisitions.

QUESTION 75

A security administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpoints:

Full disk encryption

* Password policies Application allow listing

* Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Answer: C,D

To address the specific OS benchmark configurations, the following solutions are most appropriate: C . SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

D . SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

Reference:

CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

"Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintainedeffectively.

QUESTION 76

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

Answer: D. Configure automated Isolation of human resources systems B

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

Company A and Company D ate merging Company A's compliance reports indicate branchprotections 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

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

Answer: D. If role-based training is deployed C

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.

Reference:

CompTIA SecurityX Study Guide OWASP Testing Guide

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

A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic. Which ofthe following should the analyst use to determine whether the requests are malicious?

A. User-agent string

B. Byte length of the request

C. Web application headers

Answer: D. HTML encoding field A

The user-agent string can providevaluable information to distinguish between legitimate and botrelated traffic. It contains details about the browser, device, and sometimes the operating system of

the client making the request.

Why Use User-Agent String?

Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

B . Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

C . Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

D . HTML encoding field: This is not typically used for identifying the nature of the request. Reference:

CompTIA SecurityX Study Guide

"User-Agent Analysis for Security," OWASP

NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

QUESTION 79

An organization is required to

* Respond to internal andexternal inquiries in a timely manner

* Provide transparency.

* Comply with regulatory requirements

The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

B. Integrating automated response mechanisms into the data subject access request process

C. Developing communication templates that have been vetted by internal and external counsel

D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Answer: C

Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and provide transparency in the event of a breach.

Why Communication Templates?

Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.

Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements.

Consistent Messaging: Ensures that all responses are consistent, clear, and accurate, maintaining the organizations credibility.

Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately.

Other options, while useful, do not provide the same level of preparedness and compliance:

A . Outsourcing to an external consultant: This may delay response times and lose internal control over the communication.

B . Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.

D . Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide" ISO/IEC 27002:2013, "Information technology ” Security techniques ” Code of practice for information security controls"

QUESTION 80

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

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

A. The Dl 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

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.

QUESTION 81

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?

B. HIDS and vTPM

C. WAF and syslog

Answer: D. HIPS and host-based firewall D

To meet the requirements of having allendpoints 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.

Reference:

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.

QUESTION 82

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

A. Compliance tracking

B. Situational awareness

C. Change management

D. Quality assurance

Answer: C

To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

Reference:

CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining

ITIL (InformationTechnology Infrastructure Library) Framework: Provides best practices for change management in IT services.

"The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

QUESTION 83

An audit finding reveals that a legacy platform has not retained loos for more than 30 days The platform has been segmented due to its interoperability with newer technology. As a temporarysolution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

A. Configure a scheduled task nightly to save the logs

B. Configure event-based triggers to export the logs at a threshold.

C. Configure the SIEM to aggregate the logs

D. Configure a Python script to move the logs into a SQL database.

Answer: C

To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes.

Reference:

CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention. NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis. "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

QUESTION 84

A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

A. Dark web monitoring

B. Threat intelligence platform

C. Honeypots

Answer: D. Continuous adversary emulation B

Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.

Why a Threat Intelligence Platform?

Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionableinsights.

Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.

Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.

Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.

Other options, while valuable, do not offer the same level of integration and operationalization capabilities:

A . Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive operationalization.

C . Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.

D . Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.

Reference:

CompTIA SecurityX Study Guide

"Threat Intelligence Platforms," Gartner Research

NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

QUESTION 85

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

A. Encryption systems based on large prime numbers will be vulnerable to exploitation

B. Zero Trust security architectures will require homomorphic encryption.

C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques

Answer: D. Quantum computers willenable malicious actors to capture IP traffic in real time A

Advancements in quantum computing pose a significant threat to current encryption systems,

A. Quantum

computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.

Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of thismathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.

C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.

D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes" "Quantum Computing and Cryptography," MIT Technology Review

QUESTION 86

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

Answer: D. Add the VPN hostname as a SAN entry on the root certificate A

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.

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:

CompTIASecurityX Study Guide

"Device Certificates for VPN Access," Cisco Documentation NIST Special Publication 800-77, "Guide to IPsec VPNs"

QUESTION 87

A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository The security team needs to be able to quickly evaluate whether to respond to a given vulnerability Which of the following, will allow the security team to achieve the objective with the last effort?

A. SAST scan reports

B. Centralized SBoM

C. CIS benchmark compliance reports

Answer: D. Credentialed vulnerability scan B

A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in aprivate repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.

Why Centralized SBoM?

Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.

Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.

Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.

Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.

Other options, while useful, do not provide the same level of comprehensive and efficient

A . SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.

C . CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.

D . Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.

Reference:

CompTIA SecurityX Study Guide

"Software Bill of Materials (SBoM)," NIST Documentation "Managing Container Security with SBoM," OWASP

QUESTION 88

A security engineer performed a code scan that resulted in many false positives. The security engineer must find asolution 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

Answer: D. Performing updates on code libraries before code development A

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 ofthe 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.

QUESTION 89

A security engineer needs 10 secure the OT environment based on me following requirements Isolate the OT network segment

Apply security updates two workstations Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meetthese 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: B

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host inthe 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.

QUESTION 90

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

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 beforgotten.

"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.

QUESTION 91

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: B

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.

Reference:

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.

QUESTION 92

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 arc the most appropriate? (Select two).

A. Federation

B. Microsegmentation

C. CASB

D. PAM

E. SD-WAN

F. SASE

Answer: C,F

To provide secure access tointernal 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.

Reference:

CompTIA SecurityX Study Guide

"CASB: Cloud Access Security Broker," Gartner Research

QUESTION 93

During a gap assessment, an organization notes that OYOD usage is asignificant 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 bÂ»Â« reduce the risk of OYOD devices? (Select two).

A. Cloud 1AM 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

Answer: F. DLP, to enforce data protection capabilities B,C

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):

DeviceConfiguration 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.

F . DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

Reference:

CompTIA SecurityX Study Guide

"Conditional Access Policies," Microsoft Documentation "Network Access Control (NAC)," Cisco Documentation

QUESTION 94

Audit findings indicate several user endpoints are not utilizing full disk encryption During me 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 me 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.

Answer: E. The HSM does not support sealing storage D

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.

Other options do not directly address the requirement for TPM in supporting full disk encryption:

A . The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption.

B . The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.

C . The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.

E . The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

CompTIA SecurityX Study Guide

"Trusted Platform Module (TPM) Overview," Microsoft Documentation "BitLocker Deployment Guide," Microsoft Documentation

QUESTION 95

A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Beavailable 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

Answer: D. Create a separate network for users who need access to the application D

Creating a separate network for users who need access tothe application is the best action to secure an internal application that is critical to the production area and cannot be updated.

Why Separate Network?

Network Segmentation: Isolates the critical application from the rest of the network, reducing the risk of compromise and limiting the potential impact of any security incidents.

Controlled Access: Ensures that only authorized users have access to the application, enhancing security and reducing the attack surface.

Minimized Risk: Segmentation helps in protecting the application from vulnerabilities that could be exploited from other parts of the network.

Other options, while beneficial, do not provide the same level of security for a critical application:

A . Disallow wireless access: Useful but does not provide comprehensive protection.

B . Deploy intrusion detection capabilities using a network tap: Enhances monitoring but does not provide the same level of isolation and control.

C . Create an acceptable use policy: Important for governance but does not provide technical security controls.

Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-125, "Guide to Security for Full Virtualization Technologies" "Network Segmentation Best Practices," Cisco Documentation

QUESTION 96

Asoftware company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of

A. Misconfigured code commit

B. Unsecure bundled libraries

C. Invalid code signing certificate

D. Data leakage

Answer: B

The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled

libraries. When developing and deploying new applications, it is common for developers to use thirdparty libraries. If these libraries are not properly vetted for security, they can introduce

vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?

Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.

Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.

Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.

Other options, while relevant, are less likely to cause widespread anti-malware alerts:

A . Misconfigured code commit: Could lead to issues but less likely to trigger anti-malware alerts.

C . Invalid code signing certificate: Would lead to trust issues but not typically anti-malware alerts.

D . Data leakage: Relevant for privacy concerns but not directly related to anti-malware alerts. Reference:

CompTIA SecurityX Study Guide "Securing Open Source Libraries," OWASP

"Managing Third-Party Software Security Risks," Gartner Research

QUESTION 97

A senior security engineer flags me following log file snippet as hawing likely facilitated an attacker's lateral movement in a recent breach:

Which of the following solutions, if implemented, would mitigate the nsk of this issue reoccurnnp?

A. Disabling DNS zone transfers

B. Restricting DNS traffic to UDP'W

C. Implementing DNS masking on internal servers

Answer: D. Permitting only clients from internal networks to query DNS A

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.

Reference:

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.

QUESTION 98

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

Answer: D. Writing non-zero, random data to all cells of the SSD C

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.

Reference:

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.

QUESTION 99

A security engineer is given the following requirements:

An endpoint must only execute Internally signed applications Administrator accounts cannot install unauthorized software. Attempts to run unauthorized software must be logged Which of the following best meets these requirements?

A. Maintaining appropriate account access through directory management and controls

B. Implementing a CSPM platform to monitor updates being pushed to applications

C. Deploying an EDR solution to monitor and respond to software installation attempts

Answer: D. Configuring application control with blocked hashes and enterprise-trusted root certificates D

To meet the requirements of only allowing internally signed applications, preventing unauthorized software installations, and logging attempts to run unauthorized software, configuring application control with blocked hashes and enterprise-trusted root certificates is the best solution. This approach ensures that only applications signed by trusted certificates are allowed to execute, while all other attempts are blocked and logged. It effectively prevents unauthorized software installations by restrictingexecution to pre-approved applications.

Reference:

CompTIA SecurityX Study Guide: Describes application control mechanisms and the use of trusted certificates to enforce security policies.

NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends application whitelisting and execution control for securing endpoints. "The Application Security Handbook" by Mark Dowd, John McDonald, and Justin Schuh: Covers best practices for implementing application control and managing trusted certificates

QUESTION 100

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 tobypass 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

Answer: D. Several users have not configured their mobile devices toreceive OTP codes B

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. Reference:

CompTIA SecurityX Study Guide

QUESTION 101

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:

Which of the following is the bÂ«Â« way to fix this issue?

A. Rewriting any legacy web functions

B. Disabling all deprecated ciphers

C. Blocking all non-essential pons

Answer: D. Discontinuing the use of self-signed certificates D

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

A security analystreviews 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

The table shows detailed information about products, includinglocation, 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. Reference:

CompTIA SecurityX Study Guide

NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

"Supply Chain Security Best Practices," Gartner Research

QUESTION 103

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	10.200.5.76/24	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	10.200.4.139/24	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

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 usersbeing 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.

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 bÂ«st solve this issue?

A. Rule based

B. Time-based

C. Role based

Answer: D. Context-based D

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.

QUESTION 105

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

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 nave been associated with high-risk activity.

Answer: D

The log-in activity indicates a security threat, particularly involving the ADMIN account with a highrisk 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.

Reference:

CompTIA SecurityX guide on incident response and account management. Best practices for handling compromised accounts.

Automation tools and techniques for security operations centers (SOCs).

QUESTION 106

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

A. Assessing log inactivities 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

Answer: D. Baselining user behavior to support advancedanalytics A

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.

QUESTION 107

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)

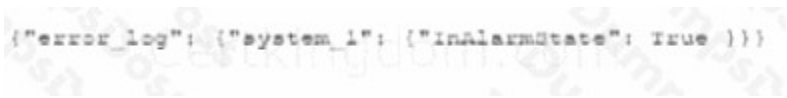
```
["error_log]
    ["system_1"]
        ["InAlarmState": True]
```

B)

```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```

C)

D)



A. Option A

B. Option B

C. Option C

Answer: D. Option D A

The code function provided in the question seems tobe 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.

Reference: CompTIA SecurityX Study Guide, Chapter on Log Management and Automation, Section on Parsing Structured Logs.

QUESTION 108

An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

A. Secure zone architecture

B. Always-on VPN

C. Accurate asset inventory

Answer: D. Microsegmentation D

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.

QUESTION 109

A company detects suspicious activity associated with external connections Security detection tools are unable tocategorize 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

Answer: D. implement UEBA D

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).

QUESTION 110 SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from companys privileged network.

The companys 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 by 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.

Answer: See explanation below.

10.1.45.65 SFTP ServerDisable 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

QUESTION 111 SIMULATION

A product development team has submitted code snippets for review prior to release.

INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet. Code Snippet 1

Code Snippet 1 Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
...
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
...
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:

SQL injection

Cross-site request forgery Server-side request forgery Indirect object reference Cross-site scripting

Fix 1:

Perform input sanitization of the userid field. Perform output encoding of queryResponse, Ensure usex:ia belongs to logged-in user.

Inspect URLS and disallow arbitrary requests. Implementanti-forgery tokens.

Vulnerability 2

1) Denial of service

2) Command injection

3) SQL injection

5) Credentials passed via GET Fix 2

A) Implement prepared statements and bind variables.

B) Remove the serve_forever instruction.

C) Prevent the "authenticated" value from being overridden by a GET parameter.

D) HTTP POST should be used for sensitive parameters.

E) Perform input sanitization of the userid field.

Answer: See the solution below in explanation.

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection byvalidating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query.

Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values. Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such

as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the users browser can be accepted by the server.

QUESTION 112 SIMULATION

A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

The PostgreSQL server must only allow connectivity in the 10.1.2.0 subnet.

The SSH daemon on the database server must be configured to listen to port 4022.

The SSH daemon must only accept connections from a Single workstation.

All host-based firewalls must be disabled on all workstations.

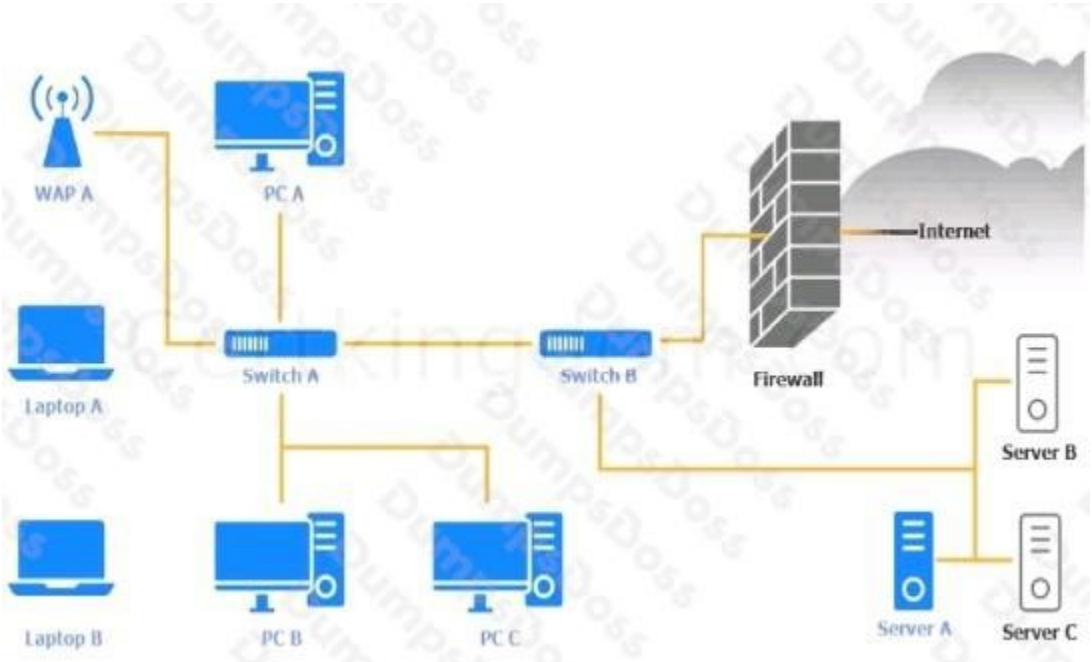
All devices must have the latest updates from within the past eight days.

All HDDs must be configured to secure data at rest. Cleartext services are not allowed.

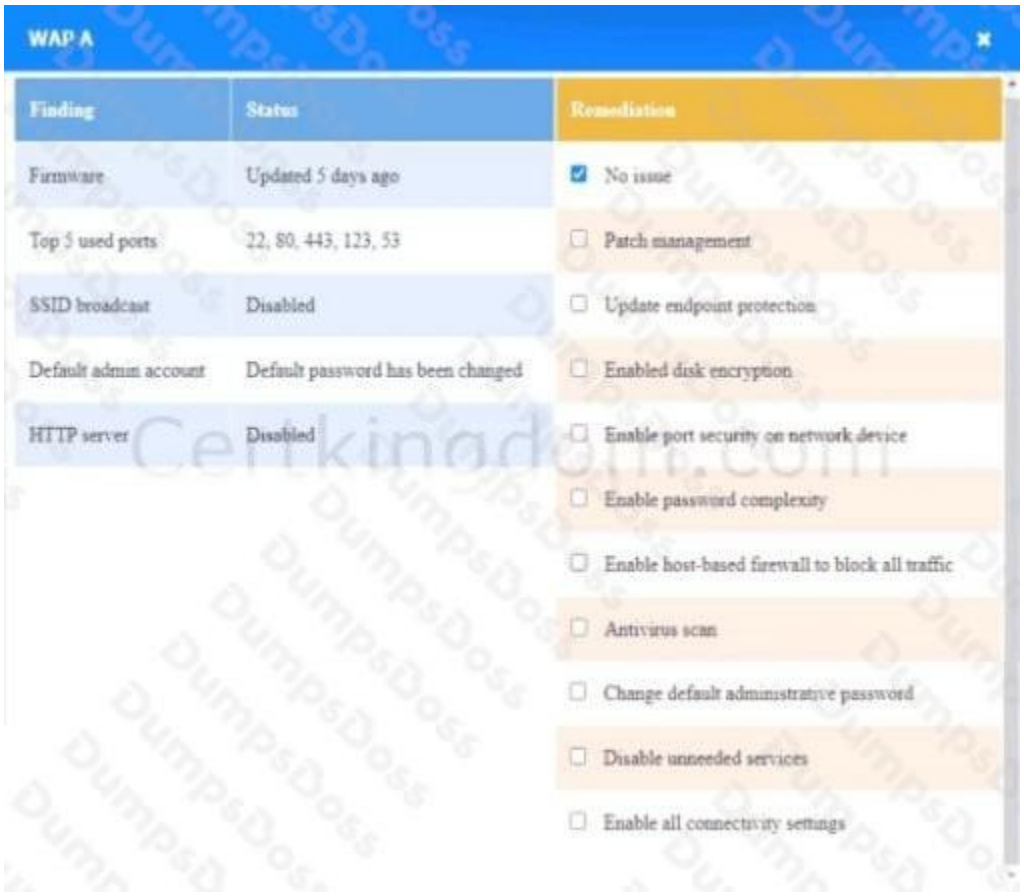
All devices must be hardened when possible. Instructions:

Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

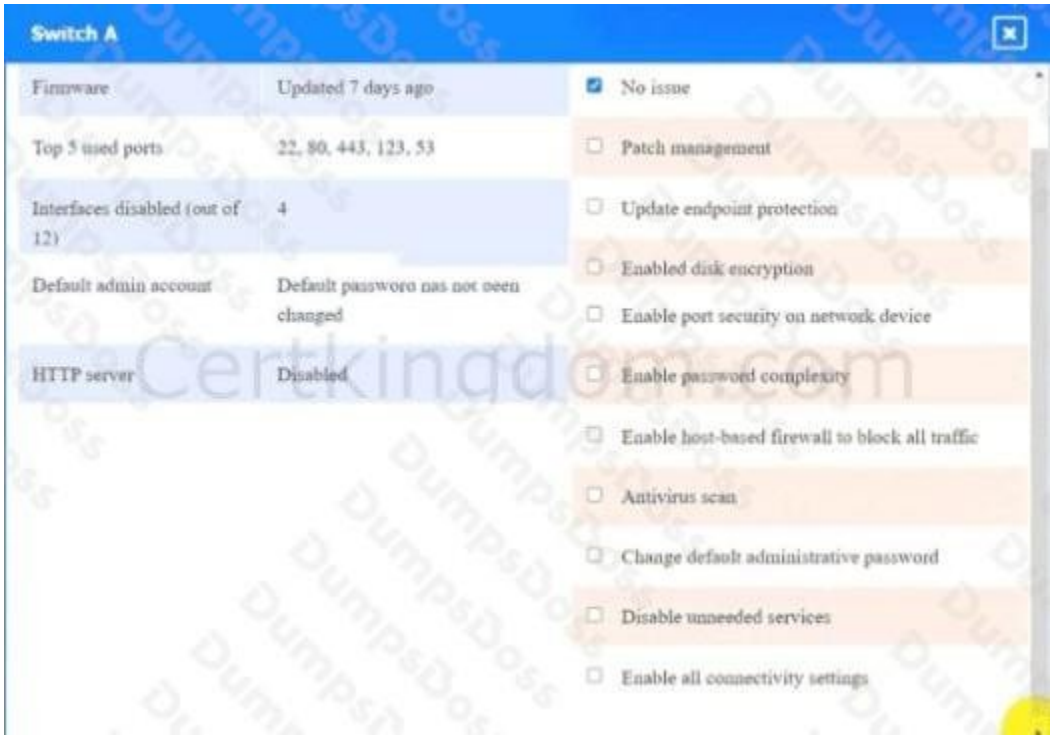

WAP A
Finding
Status
Remediation
Firmware
Updated 5 days ago
No issue
Top 5 used ports
22, 80, 443, 123, 53
Patch management
SSID broadcast
Disabled
Update endpoint protection
Default admin account
Default password has been changed
Enabled disk encryption
HTTP server
Disabled
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

PC A

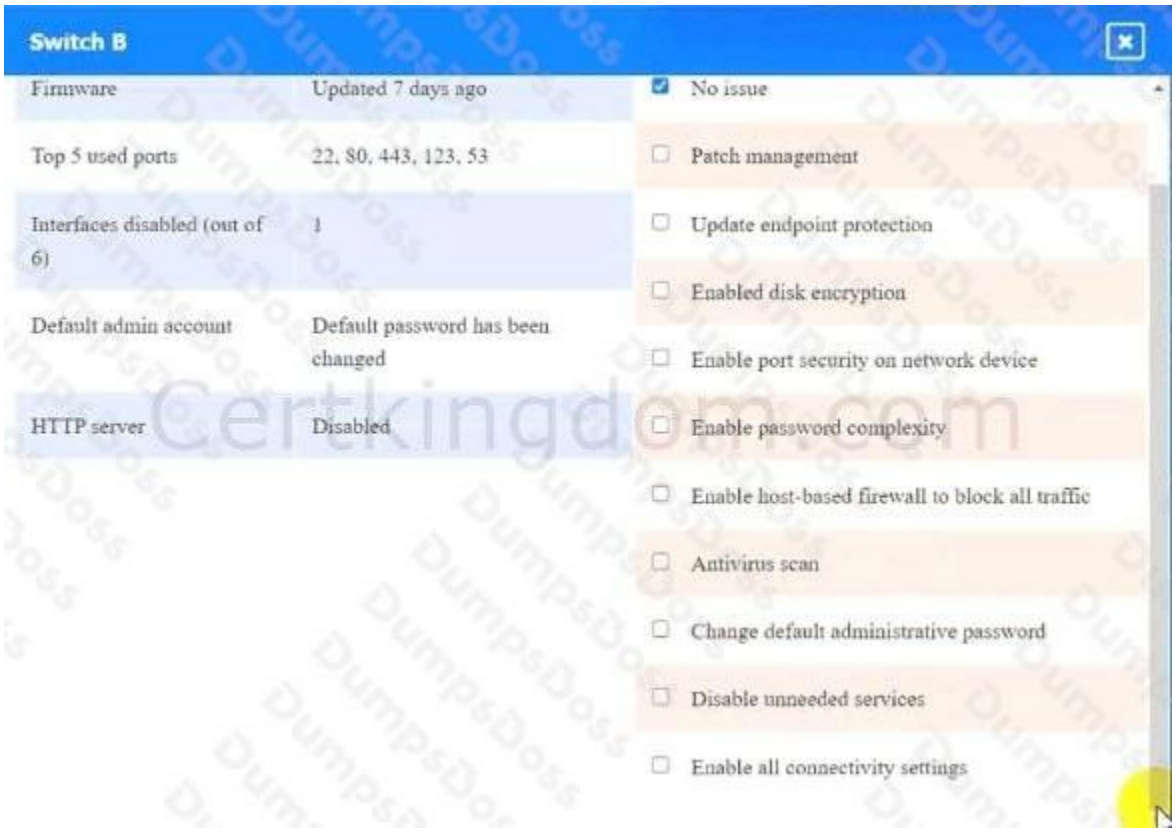

PC A
OS updates
Updated 2 days ago, last checked 5:08 a.m.
No issue
Endpoint protection
Last checked 6:11 a.m.
Patch management
Browser version
91.2.5 (7/31/2023)
Update endpoint protection
Disk encryption
Enabled
Enabled disk encryption
Password complexity
Enabled
Enable port security on network device
Host-based firewall
Disabled
Enable password complexity
CPU & memory usage
Normal
Enable host-based firewall to block all traffic
Screensaver
Enabled
Antivirus scan
Top 5 used ports
22, 80, 443, 389, 53
Change default administrative password
Wireless
Disabled
Disable unneeded services
Enable all connectivity settings

Laptop A

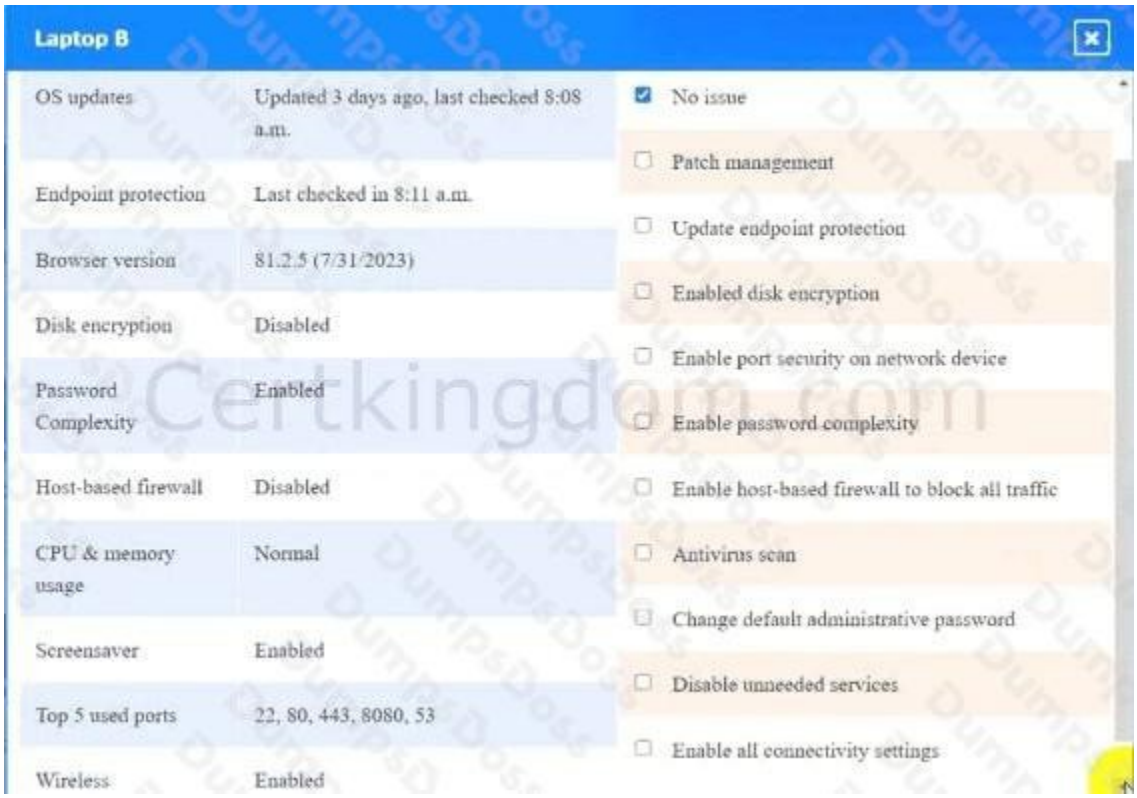
Switch A



Switch B:


Switch B
Firmware
Updated 7 days ago
Top 5 used ports
22, 80, 443, 123, 53
Interfaces disabled (out of 6)
1
Default admin account
Default password has been changed
HTTP server
Disabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

Laptop B


Laptop B
OS updates
Updated 3 days ago, last checked 8:08 a.m.
Endpoint protection
Last checked in 8:11 a.m.
Browser version
81.2.5 (7/31/2023)
Disk encryption
Disabled
Password Complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
Normal
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 8080, 53
Wireless
Enabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

PC B


PC B
OS updates
Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection
Last checked in 6:13 a.m.
Browser version
91.2.5 (7/31/2023)
Disk encryption
Enabled
Password complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
Medium
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 389, 53
Wireless
Disabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

PC C


PC C
OS updates
Updated 22 days ago
Endpoint protection
Last checked 6:19 a.m.
Browser version
91.2.5 (7/18/2022)
Disk encryption
Enabled
Password complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
High
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 23, 53
Wireless
Disabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

Server A


Server A
Nmap
IP Tables
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.4
80/tcp closed http
443/tcp closed ssl/http
1433/tcp closed mssql
5432/tcp closed postgresql
...
1 2 3 4
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
1 2 3 4
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
1 2 3 4
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
1 2 3 4
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT

Answer: See the Explanation below for the solution.

WAP A: No issue found. The WAP A is configured correctly and meets therequirements. PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network.

However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management

This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop

A. However, this option may also require a reboot of Laptop A

and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.

Switch A: No issue found. The Switch A is configured correctly and meets the requirements. Switch B: No issue found. The Switch B is configured correctly and meets the requirements. Laptop B: Disable unneeded services

This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to

PC B: Enable disk encryption

This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC Bs data. However, this option

may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.

PC C: Disable unneeded services

This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is thedefault and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the

functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:

sudo nano /etc/ssh/sshd_config Server

A. Need to select the following:

A black and white screen with white text Description automatically generated

QUESTION 113 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 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.

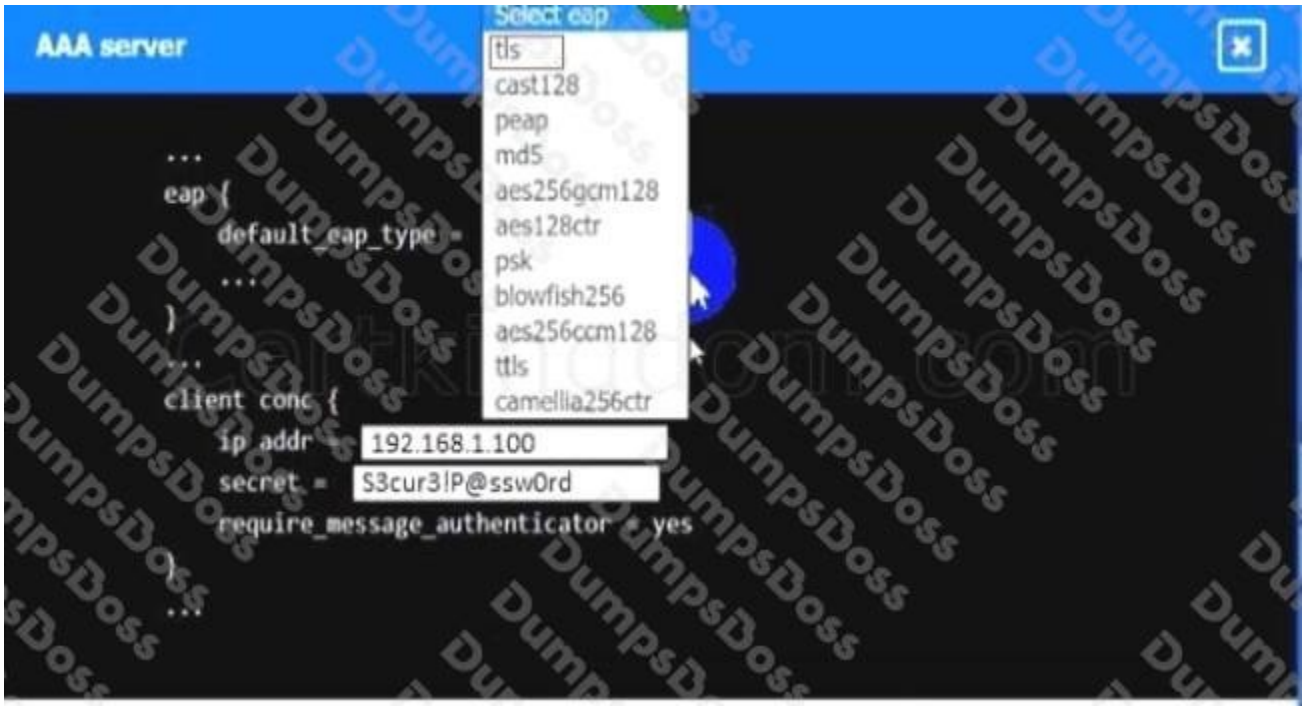
VPN Concentrator:

AAA Server:

Answer: See the answer below in Explanation.

VPN Concentrator:

A screenshot of a computer Description automatically generated AAA Server:



A screenshot of a computer Description automatically generated

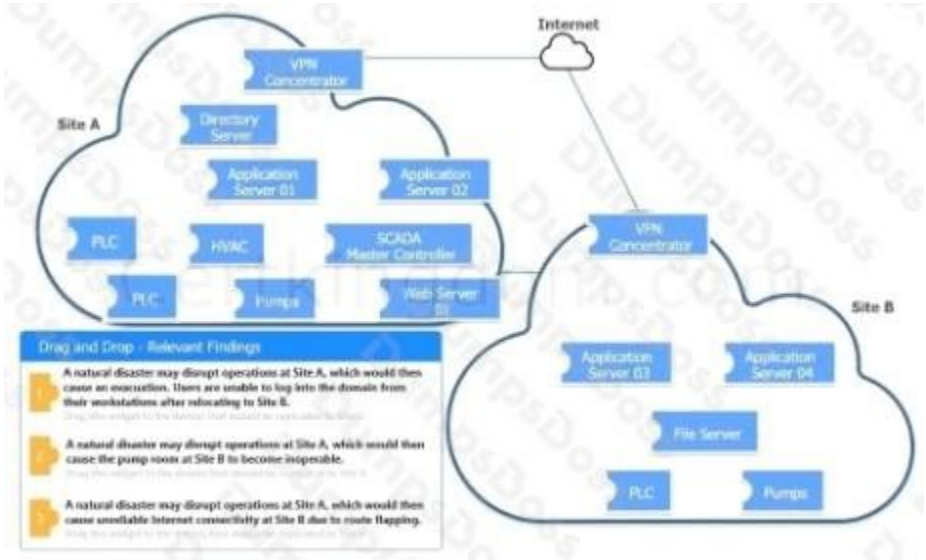
QUESTION 114 DRAG DROP

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 simul-ation, please click the Reset All button.



Answer:

A computer screen shot of a diagram Description automatically generated

A screenshot of a computer

error Description automatically generated

QUESTION 115 SIMULATION

An organization is planning for disaster recovery and continuity ofoperations, 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.

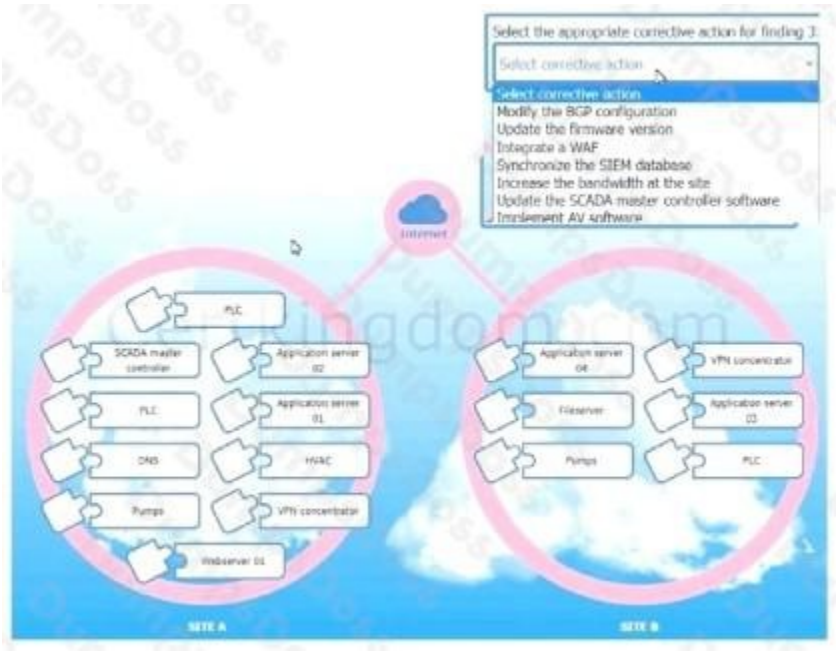
3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.

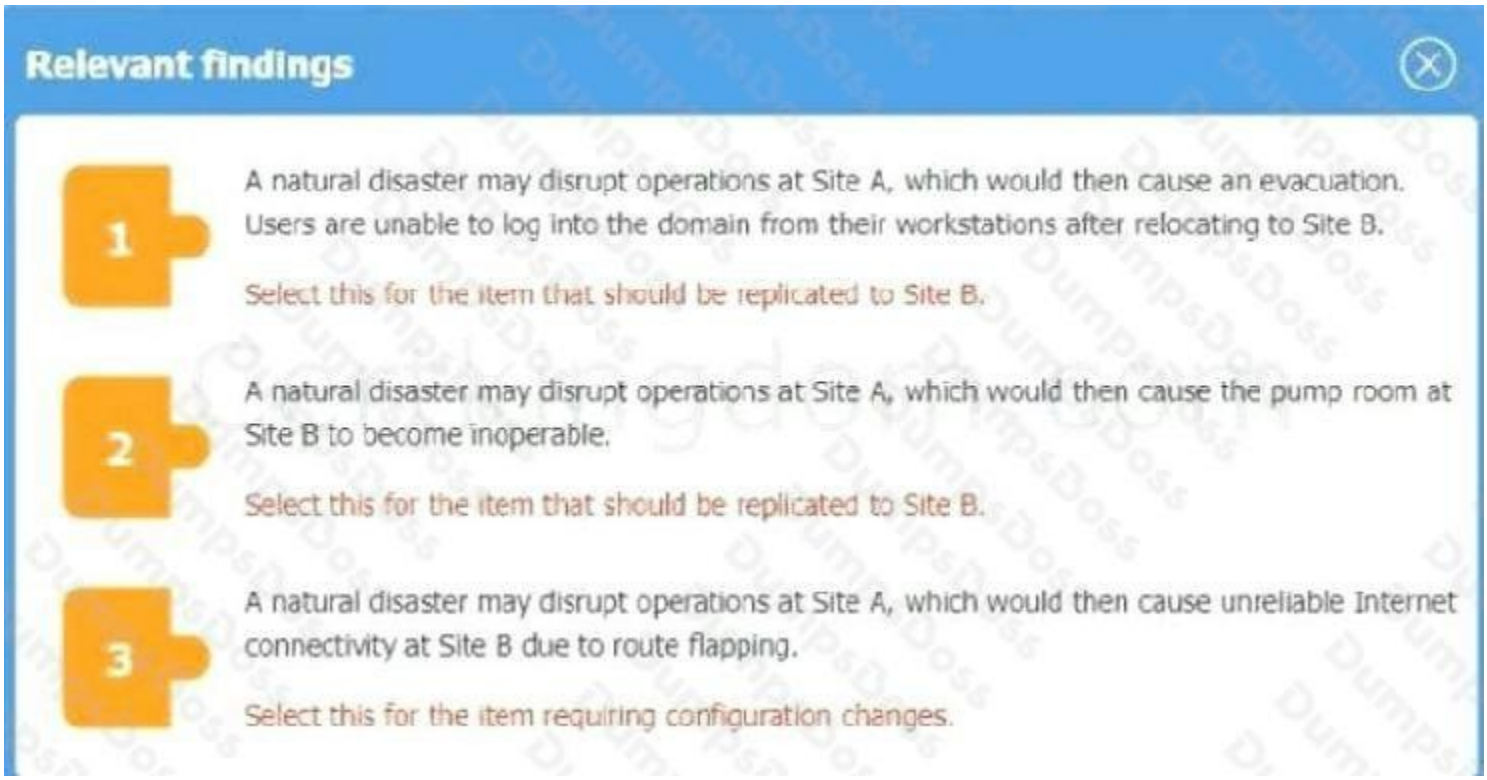
INSTRUCTIONS

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.





Answer: See the complete solution

below in

Matching Relevant Findings to the Affected Hosts:

Finding 1:

Affected Host: DNS

Finding 2:

Affected Host: Pumps

Finding 3:

Affected Host: VPN Concentrator

Corrective Actions for Finding 3:

Finding 3 Corrective Action:

Action: Modify the BGP configuration

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.

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.

QUESTION 116 SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.


IoC 1
IoC 2
IoC 3
Source Svc Type Dest Data
Apache_httpd DNSQ @10.1.1.1:53 update.s.domain
Apache_httpd DNSQR @10.1.2.5 CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd DNSQ @10.1.1.1:53 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd DNSQR @10.1.2.5 IN A 108.158.253.253
Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Analysis
Select analysis
Remediation
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation


IoC 1
IoC 2
IoC 3
Src Dst Proto Data Action
10.0.5.5 10.1.2.1 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.2 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.3 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.4 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.5 IP_ICMP ECHO Drop
Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Analysis
Select analysis
Remediation
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation

Answer: See the complete solution below in

Analysis and Remediation Options for Each IoC:

IoC 1:

Evidence:

Source: Apache_httpd Type: DNSQ

Dest: @10.1.1.1:53,@10.1.2.5

Data: update.s.domain, CNAME 3a129sk219r9slmfkzzz000.s.domain, 108.158.253.253 Analysis:

Analysis: The service is attempting to resolve a malicious domain.

Remediation:

Remediation: Implement a blocklist for known malicious ports.

domains, thereby protecting the network from potential connections to malicious servers. IoC 2:

Evidence:

Src: 10.0.5.5

Dst: 10.1.2.1, 10.1.2.2, 10.1.2.3, 10.1.2.4, 10.1.2.5

Proto: IP_ICMP Data: ECHO Action: Drop Analysis:

Analysis: Someone is footprinting a network subnet.

Remediation:

Remediation: Block ping requests across the WAN interface.

IoC 3:

Evidence:

Proxylog:

GET

/announce?info_hash=%01dff%27f%21%10%c5%wp%4e%1d%6f%63%3c%49%6d&peer_id%3dxJFS Uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started

User-Agent: RAZA 2.1.0.0 Host: localhost Connection: Keep-Alive HTTP200 OK

Analysis:

Analysis: An employee is using P2P services to download files.

Remediation:

Remediation: Enforce endpoint controls on third-party software installations.

Reference:

CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

QUESTION 117 SIMULATION

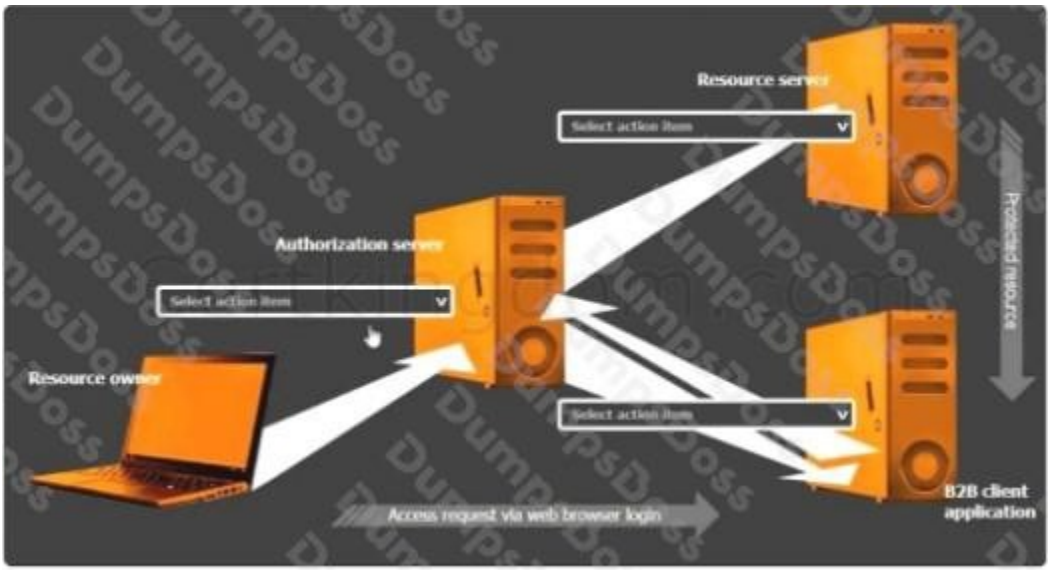
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

. The application does not need to know the users' credentials.

. An approval interaction between the users and theHTTP 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: See the complete solution below in

Select the Action Items for the Appropriate Locations:

Authorization Server:

Action Item: Grant access

The authorization server's role is to authenticate the user and then issue an authorization code or token that the client application can use to access resources. Granting access involves the server authenticating the resource owner and providing the necessary tokens for the client application. Resource Server:

Action Item: Access issued tokens

The resource server is responsible for serving the resources requested by the client application. It must verify the issued tokens from the authorization server to ensure the client has the right permissions to access the requested data.

B2B Client Application:

Action Item: Authorize access to other applications

The B2B client application must handle the OAuth flow to authorize access on behalf of the user without requiring direct knowledge of the user's credentials. This includes obtaining authorization tokens from the authorization server and using them to request access to the resource server.

Detailed

OAuth 2.0 is designed to provide specific authorization flows for web applications, desktopapplications, mobile phones, and living room devices. The integration involves multiple steps and components, including:

Resource Owner (User):

Requests access to the resources controlled by the resource owner but does not directly handle the user's credentials. Instead, it uses tokens obtained through the OAuth flow.

Authorization Server:

Handles the authentication of the resource owner and issues the access tokens to the client application upon successful authentication.

Resource Server:

Hosts the resources that the client application wants to access. It verifies the access tokens issued by the authorization server before granting access to the resources.

OAuth Workflow:

The resource owner accesses the client application.

The client application redirects the resource owner to the authorization server for authentication. The authorization server authenticates the resource owner and asks for consent to grant access to the client application.

Upon consent, the authorization server issues an authorization code or token to the client application.

The client application uses the authorization code or token to request access to the resources from the resource server.

The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.

Reference:

CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.

OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.

OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy-to-understand explanation of the OAuth 2.0 protocol.

By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

QUESTION 118

An endpoint security engineer finds that a newly acquired company has a variety of non-standard applications running and no defined ownership for those applications. The engineer needs to find a solution thatrestricts malicious programs and software from running in that environment, while allowing the non-standard applications to function without interruption. Which of the following application control configurations should the engineer apply?

A. Deny list

B. Allow list

Answer: D. MAC list C

Step-by-Step Option A: Deny list

Deny lists block specific applications or processes identified as malicious.

This approach is reactive and mayinadvertently block the non-standard applications that are currently in use without proper ownership.

Option B: Allow list

Allow lists permit only pre-approved applications to run.

While secure, this approach requires defining all non-standard applications, which may disrupt operations in an environment where ownership is unclear.

Option C: Audit mode Correct Answer.

Audit mode allows monitoring and logging of applications without enforcing restrictions.

This is ideal in environments with non-standard applications and undefined ownership because it enables the engineer to observe the environment and gradually implement control without interruption.

Audit mode provides critical visibility into the software landscape, ensuring that necessary applications remain functional.

Option D: MAC list

Mandatory Access Control (MAC) lists restrict access based on classification and clearance levels. This does not align with application control objectives in this context.

CompTIA CASP+ Study Guide - Chapters on Endpoint Security and Application Control. CASP+ Objective 2.4: Implement appropriate security controls for enterprise endpoints.

QUESTION 119

Embedded malware has been discovered in a popular PDF reader application and is currently being exploited in the wild. Because the supply chain was compromised, this malware is present in versions

10.0 through 10.3 of the software's official versions. The malware is not present in version 10.4. Since the details around this malware are still emerging, the Chief Information Security Officer has asked the senior security analyst to collaborate with the IT asset inventory manager to find instances of the installed software in order to begin response activities. The asset inventory manager has asked an analyst to provide a regular expression that will identify the affected versions. The software installation entries are formatted as follows:

Reader 10.0

Reader 10.1

Reader 10.2

Reader 10.3

Reader 10.4

Which of the following regular expression entries will accuratelyidentify all the affected versions?

A. Reader(*)[1][0].[0-4:

B. Reader[11[01X.f0-3'

C. Reader( )[1][0].[0-3:

D. Reader( )[1][0] X.[1-3:

Answer: C

Step-by-Step

Understand the QuestionRequirements:The goal is to use a regular expression (regex) to match software versions 10.0 through 10.3, but exclude version 10.4.

Review Regex Syntax:

[ ] indicates a character set (matches any one character in the set). [0-3] matches any digit between 0 and 3.

\. escapes the period (.) so it matches a literal period instead of acting as a wildcard. ( ) groups parts of the regex together.

Analyze Each Option:

Option A: Reader(*)[1][0].[0-4:

Incorrect. The use of (*) is not valid syntax in this context and [0-4 is incomplete or misformatted. Option B: Reader[11[01X.f0-3'

Incorrect. This is an invalid regex syntax, mixing character sets and mismatched brackets. Option C: Reader( )[1][0].[0-3:

Correct. This regex is valid and matches "Reader 10.0", "Reader 10.1", "Reader 10.2", and "Reader 10.3" while excluding "Reader 10.4".

Breakdown:

Reader: Matches the text "Reader".

[1][0]: Matches "10" as a combination of two characters.

\.: Matches the literal period.

[0-3]: Matches any single digit between 0 and 3. Option D: Reader( )[1][0] X.[1-3:

Incorrect. The syntax X.[1-3 is invalid, and this does not match the required versions. Conclusion:The regex in Option C correctly identifies all affected versions (10.0, 10.1, 10.2, 10.3) while excluding the unaffected version (10.4).

Reference:

CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter on Vulnerability Management.

CompTIA CASP+ Exam Objectives: "Analyze risks associated with new vulnerabilities." Regular Expressions Documentation from CASP+ Official Reference Materials.

QUESTION 120

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. Passthe-hash attack

Answer: A

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:

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

Reference: CASP+ objectives often emphasize supply chain security due to its growing importance. The scenario directly relates to this type of attack, as the registry helps ensure that software packages haven't been tampered with during the supply chain process.

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 theprimary 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.

Answer: Why A is the Correct

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.

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.

QUESTION 121

An organization is implementing advanced security controls associated with the execution of software applications on corporate endpoints. The organization must implement a deny-all, permitby-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

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

Reference: SELinux is a powerful tool often covered in CASP+ material, but its OS-specific nature makes it unsuitable here.

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).

Reference: MDM is relevant to CASP+ in the context of mobile security, but it's not the best fit for this cross-platform application control requirement.

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 controlpolicies.

Reference: XDR is a key component of modern security architectures and is covered in CASP+, but its focus is threat detection, not preventative application control.

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.

Reference: Allow lists (whitelisting) are a fundamental security control emphasized in CASP+. They are a core component of application control strategies.

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.

In conclusion, an allow list (application whitelisting) is the most appropriate solution to implement a "deny-all, permit-by-exception" application control policy across all operating systems. It's a powerful security control aligned with the principles of least privilege and is a core concept covered in the CASP+ exam objectives. It is implied that the question was intended to be Allow List, but as written, Block List is the only reasonable answer.

QUESTION 122

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: A

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 weredesigned to operate in air-gapped environments, completely isolated from external networks (including the internet).

Reference: This aligns with the historical evolution of OT security. Initially, security was based on physical isolation rather than network security controls. This is a common topic in CASP+ discussions on OT security challenges.

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.

Answer: Why A is the Correct

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.

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.

==========

QUESTION 123

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

Answer: D. Encrypting using a key escrow process for storage of the encryption key A

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 thebest option for maintaining complete control over encryption keys. An HSM is a dedicated, tamperresistant 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.

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.

Answer: Why A is the Correct

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.

==========

QUESTION 124

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

Step by Step

Understanding the Scenario: Theorganization 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 cloudmanaged 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.

Answer: Why B is the Correct

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

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.

QUESTION 125

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

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 PreventionSystems (NIPS) (D) focuses on network

traffic, not application-layer security.

QUESTION 126

A security officer performs due diligence activities before implementing a third-party solution into the enterprise environment. The security officer needs evidence from the third party that a data subject access request handling process is in place. Which of the following is the security officer most likely seeking to maintain compliance?

A. Information security standards

B. E-discovery requirements

D. Certification requirements

Answer: E. Reporting frameworks C

Step-by-Step

Privacy regulations (C), such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), require companies to provide data subject access request (DSAR) handling processes. A DSAR allows individuals to request details about their personal data stored by a company and request modifications or deletions.

Information security standards (A) focus on overall security controls, while e-discovery requirements

(B) relate to legal investigations rather than ongoing compliance.

QUESTION 127

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.islpv4()) { 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.

D. Sample 1 is the target agent while Sample 2 is the C2 server.

Answer: B

Step-by-Step

Both samples share similar function names, variable naming styles, and logic flow, indicating that they were likely written by the same developer. This is a keyobservation in malware attribution, as cyber threat analysts often look for unique coding styles to link malware to specific threat actors. The presence of C2 (Command and Control) communication in both samples supports this theory, as attackers often reuse parts of their own malware code across different attacks.

QUESTION 128

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

Answer: D. Rita A

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.

QUESTION 129

A company reduced its staff 60 days ago, and applications are now starting to fail. The security analyst is investigating to determine if there is malicious intent for the application failures. The security analyst reviews the following logs:

22:03:50 sshd[21502]: Success login for user01 from 192.168.2.5 22:10:00 sshd[21502]: Failed login for user10 from 192.168.2.5 22:11:40 sshd[21502]: Success login for user07 from 192.168.2.58 22:12:00 sshd[21502]: Failed login for user10 from 192.168.2.5 22:13:00 sshd[21502]: Failed login for user10 from 192.168.2.5

Which of the following is the most likely reason for the application failures?

A. The users account was set as a service account.

B. The user's home directory was deleted.

C. The user does not have sudo access.

D. The root password has been changed.

Answer: B

The logs indicate multiple failed login attempts for user10, who may have been part of the staff

reduction 60 days prior. If user10's account was removed, and their home directory deleted, any applications or services relying on files or configurations within that directory would fail. This scenario is common when service accounts are not properly identified and preserved during staff reductions.

Ensuring that service accounts are documented and maintained separately from user accounts is essential to prevent unintended disruptions to applications and services.

Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: "Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment."

QUESTION 130

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

Answer: D. Canary C

Step-by-Step

Regression testing ensures that new changes do not break existing functionality. It would have identified the memory leak before deployment, preventing downtime.

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

Answer: D. Interactive application security testing A

Software Composition Analysis (SCA) is the best method for identifying all components, dependencies, and open-source libraries used inan 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.

Reference: CASP+ CAS-005 Official Study Guide " Chapter on Secure Software Development

QUESTION 132

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

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:

A (File monitoring tool) helps detect file changes but doesnt 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.

Reference: CASP+ CAS-005 Official Study Guide “Security Operations and Logging

QUESTION 133

A Chief Information Security Officer is concerned about the operational impact of ransomware. In the event of a ransomware attack, the business requires the integrity of the data to remain intact and an RPO of less than one hour. Which of the following storage strategies best satisfies the business requirements?

A. Full disk encryption

B. Remote journaling

C. Immutable

D. RAID 10

Answer: B

Remote journaling continuously sends log updates to a remote system, ensuring near-real-time backup and an RPO (Recovery Point Objective) under one hour.

Key concepts:

RPO under one hour means minimal data loss.

Remote journaling provides rapid recovery by keeping near-live backups. Other options:

A(Full disk encryption) protects against unauthorized access but does not aid recovery.

C (Immutable storage) prevents modification but does not ensure real-time backups.

D (RAID 10) improves redundancy but does not help against ransomware. Reference: CASP+ CAS-005 “ Business Continuity and Disaster Recovery Planning

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

Forward secrecy (FS) ensures that past encrypted data remains secure even if encryption keys are compromised in the future. Itgenerates ephemeral session keys that are not reused.

Other options:

A (Tokenization) replaces sensitive data with tokens but does not prevent key compromise.

B (Key stretching) makes brute-force attacks harder but does not ensure secrecy after compromise. D (Simultaneous Authentication of Equals " SAE) is used in WPA3 but is not related to past communication security.

Reference: CASP+ CAS-005 " Cryptographic Concepts and Key Management

QUESTION 135

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

Implementing security and quality checks in a CI/CD pipeline ensures that: Container images are scanned for vulnerabilities beforedeployment.

Version control is enforced, preventing unauthorized changes. Hashes validate image integrity.

Other options:

A (Configuring ACLs on mesh networks) improves access control but does not ensure scanning.

C (Audits on container images) detect changes but do not enforce best practices.

D (Pulling from a vendor repository) does not ensure vulnerability scanning. Reference: CASP+ CAS-005 " DevSecOps and Secure Containerization

QUESTION 136

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

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

Answer: D. Coordinating the scan execution with the remediation team early in the process B

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 RiskManagement

QUESTION 137

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

Answer: D. Secure access service edge D

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.

Lets analyze the options:

A . Container orchestration: This refers to managing and automating containerized workloads (e.g., Kubernetes). While useful for application deployment, it doesnt directly address secure connectivity to cloud resources.

B . Microsegmentation: This involves creating fine-grained security policies within a network to limit lateral movement. Its valuable for internal security but isnt a complete solution for trusted

C . Conditional access: This ensures access based on conditions (e.g., user identity, device health). Its 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.

QUESTION 138

Employees use their badges to track the number of hours they work. The badge readers cannot be upgraded due to facility constraints. The software for the badge readers uses a legacy platform and requires connectivity to the enterprise resource planning solution. Which of the following is the best to ensure the security of the badge readers?

A. Segmentation

B. Vulnerability scans

Answer: C. Anti-malware A

Segmentationis the best option to ensure the security of legacy badge readers that cannot be upgraded. Segmentation isolates the legacy devices on a separate network segment to minimize their exposure to potential threats. This approach reduces the attack surface by preventing unauthorized access from other parts of the network while still allowing necessary connectivity to the enterprise resource planning (ERP) system.

Vulnerability scans (B)are useful for identifying weaknesses but do not actively protect the badge readers.

Anti-malware (C)is ineffective since the badge readers use a legacy platform that likely does not support modern endpoint protection solutions.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 2.0 (Security Architecture), Section onNetwork Segmentation & Attack Surface Management

QUESTION 139

A companys internal network is experiencing a security breach, and the threat actor is still active. Due to business requirements, users in this environment are allowed to utilize multiple machines at the same time. Given the following log snippet:

Time	User	Process	Status	Machine
10:11	user-a	.exe	blocked	machine02
10:15	user-b	setup.exe	blocked	machine02
10:15	user-A	appwiz.exe	blocked	machine01
10:16	user-c	appwiz.CPL	blocked	machine03
11:17	user-c	cmd.exe	blocked	machine03
11:18	user-h	msconfig.exe	blocked	machine04
11:19	user-d	firefox.exe	blocked	machine04
11:19	user-d	cmd.com	blocked	machine01

Which of the following accounts should a security analyst disable to best contain the incident without impacting valid users?

A. user-a

B. user-b

C. user-c

D. user-d

Answer: C

Useruser-cis showinganomalous behavior across multiple machines, attempting to run administrative tools such as cmd.exe and appwiz.CPL, which are commonly used by attackers for system modification. The activity pattern suggests a lateral movement attempt, potentially indicating a compromised account.

user-a (A)anduser-b (B)attempted to run applications but only on one machine, suggesting less likelihood of compromise.

user-d (D)was blocked running cmd.com, but user-cs pattern is more consistent with an attack technique.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section onThreat Intelligence and Indicators of Attack

A security engineer must resolve a vulnerability in a deprecated version of Python for a customdeveloped flight simul-ation application that is monitored and controlled remotely. The source code

is proprietary and built with Python functions running on the Ubuntu operating system. Version control is not enabled for the application in development or production. However, the application must remain online in the production environment using built-in features. Which of the following solutions best reduces theattack surface of these issues and meets the outlined requirements?

A. Configure code-signing within the CI/CD pipeline, update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.

B. Enable branch protection in the GitHub repository. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.

C. Use an NFS network share. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.

D. Configure version designation within the Python interpreter. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.

Answer: A

Code-signing within theCI/CD pipelineensures that only verified and signed code is deployed, mitigating the risk of supply chain attacks. Updating Python withaptitudeand updating modules withpipensures vulnerabilities are patched. Deploying the solution to production after testing maintains application availability while securing the development lifecycle.

Branch protection (B)applies only to version-controlled environments, which is not the case here. NFS network share (C)does not address the deprecated Python vulnerability.

Version designation (D)does not eliminate security risks from outdated dependencies. Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onSoftware Assurance and Secure Development

QUESTION 141

A building camera is remotely accessed and disabled from the remote console application during offhours. 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 allowconnections from approved IPs.

D. Block IP 104.18.16.29 on the firewall.

Answer: C

The logs indicate unauthorized access from104.18.16.29, an external IP, to the building cameras administrative console during off-hours.Restricting access only to approved IPsensures 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 onAccess Control and Network Security

QUESTION 142

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 PM	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	HR System	Allow
8:49 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 PM	192.168.1.5	104.18.16.29	Toronto	HR System	Deny

Which of the following is most likely the reason for the issue?

A. The user inadvertently tripped the geoblock rule in NGFW.

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

The logs show that the user connected fromToronto (104.18.16.29)andLos Angeles (95.67.137.12)within minutes. The sudden location change is a typical trigger forgeoblocking in a Next-Generation Firewall (NGFW), leading to theHR System being denied.

A compromised account (B)would show failed login attempts or unusual activities, but all other access attempts were allowed.

Business hours restriction (C)is unlikely since the user was granted access earlier. Approved subnet issues (D)would affect all applications, not just HR System access.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0(Security Operations), Section onFirewall Rules and Network Traffic Analysis

QUESTION 143

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.

Answer: C

Device attestationensures that only corporate-approved devices can perform privileged actions in SaaS applications.Continuous authorizationmonitors ongoing device compliance, dynamically adjusting permissions based onsecurity 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 onIdentity & Access Management (IAM)

QUESTION 144

A company wants to modify its process to comply with privacy requirements after an incident involving PII data in a development environment. In order to perform functionality tests, the QA team still needs to use valid data in the specified format. Which of the following best addresses the risk without impacting the development life cycle?

A. Encrypting the data before moving into the QA environment

B. Truncating the data to make it not personally identifiable

C. Using a large language model to generate synthetic data

Answer: D. Utilizing tokenization for sensitive fields D

Tokenizationreplaces sensitive data (e.g., PII) with non-sensitive placeholders while maintaining format consistency, ensuring compliancewithout disrupting testing. This method is commonly used forPCI-DSS and GDPR compliancewhile preserving data structure for functional tests.

Encryption (A)secures data but does not remove sensitivity or solve testing concerns. Truncation (B)removes portions of data but may impact testing if format requirements are strict.

Synthetic data (C)can be useful but may not always match real-world scenarios perfectly for testing purposes.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 1.0 (Governance, Risk, and Compliance), Section onPrivacy Risk Considerations & Data Protection

QUESTION 145

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

A. Enforce Secure Boot.

B. Performattack surface reduction.

C. Disable third-party integrations.

D. Limit access to the systems.

Answer: B

Attack surface reductionfocuses on minimizingunnecessary services, open ports, and vulnerabilities, reducing the exposure to potential adversaries. This aligns withzero 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. Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 2.0 (Security Architecture), Section onAttack Surface Management and Reduction

QUESTION 146

Acompany 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

Creatingsecure baseline imagesensuresconsistent, repeatabledeployment aligned with hardening standards. These images can be used acrosson-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.

QUESTION 147

A threat hunter is identifying potentially malicious activity associated with an APT. When the threat hunter runs queries against the SIEM platform with a date range of 60 to 90 days ago, the involved account seems to be typically most active in the evenings. When the threat hunter reruns the same query with a date range of 5 to 30 days ago, the account appears to be most active in the early morning. Which of the following techniques is the threat hunter using to better understand the data?

A. TTP-based inquiries

B. User behavior analytics

C. Adversary emulation

Answer: D. OSINT analysis activities B

User behavior analytics (UBA)detectsanomalousactivityby analyzing historical patterns and comparing them to recent behavior. The time shift in account activity suggestspotential compromise or misuse.

TTP-based inquiries (A)focus on known attack tactics, techniques, and procedures but do not involve behavior tracking.

Adversary emulation (C)simulates attacks but does not analyze real data trends.

OSINT analysis (D)gathers intelligence from public sources, which is unrelated to internal account behavior analysis.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section onThreat Intelligence and User Behavior Analytics (UBA)

QUESTION 148

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: B

Anacceptable 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. Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 1.0(Governance, Risk, and Compliance), Section onSecurity and Reporting Frameworks

QUESTION 149

An organization that performs real-time financial processing is implementing a new backup solution. Given the following business requirements:

The backup solution must reduce the risk of potential backup compromise. The backup solution must be resilient to a ransomware attack.

The time to restore from backups is less important than backup data integrity. Multiple copies of production data must be maintained.

Which of the following backup strategies best meets these requirements?

A. Creating a secondary, immutable database and adding 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

Answer: D. Setting up anti-tampering on the databases to ensure data cannot be changed unintentionally A

Animmutable databasepreventsmodifications or deletions, ensuring resilience against ransomware while maintaining multiple copies of data.

Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onData Protection & Backup Strategies

QUESTION 150

A company migrating to aremote work model requires that company-owned devices connect to a VPN before logging in to the device itself. The VPN gateway requires that a specific key extension is deployed to the machine certificates in the internal PKI. Which of the following best explains this requirement?

A. The certificate is an additional factor to meet regulatory MFA requirements for VPN access.

B. The VPN client selected the certificate with the correct key usage without user interaction.

D. The server connection uses SSL VPN, which uses certificates for secure communication.

Answer: B

This scenario describes anenterprise VPN setup that requires machine authenticationbefore a user logs in. The best explanation for this requirement is that theVPN client selects the appropriate certificate automaticallybased on the key extension in the machine certificate.

Understanding the Key Extension Requirement:

PKI (Public Key Infrastructure)issues machine certificates that include specific key usages such asClient AuthenticationorIPSec IKE Intermediate.

Key usage extensionsdefine how a certificate can be used, ensuring that onlyvalid certificates are selected by the VPN client.

Why Option B is Correct:

The VPNautomaticallyselects the correct machine certificate with the appropriate key extension. The process occurswithout user intervention, ensuring seamless VPN authentication before login. Why Other Options Are Incorrect:

A (MFA requirement):Certificates used in this scenario are for machine authentication, not user MFA. MFA typically involves user credentials plus a second factor (like OTPs or biometrics), which isnot applicable here.

C (Wi-Fi connectivity before login):This refers topre-logon networking, which is a separate concept where devices authenticate to a Wi-Fi network before login, usually via 802.1X EAP-TLS. However, this question specifically mentions VPN authentication, not Wi-Fi authentication.

D (SSL VPN with certificates):While SSL VPNs do use certificates,this scenario involves machine certificates issued by an internal PKI, which are commonly used inIPSec VPNs, not SSL VPNs.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide: Section onMachine Certificate Authentication in VPNs

NIST SP 800-53: Guidelines on authentication mechanisms

RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile

QUESTION 151

Anorganization has noticed an increase in phishing campaigns utilizingtyposquatting. A security analyst needs to enrich the data for commonly used domains against the domains used in phishing campaigns. The analyst uses a log forwarder to forward network logs to the SIEM. Which of the following would allow the security analyst to perform this analysis?

A. Use acron jobto regularly update and compare domains.

B. Create aparserthat matches domains.

C. Develop aquerythat filters out all matching domain names.

Answer: D

Enriching data to compare domains requires actionable visibility. Lets analyze:

A . Cron job:Automates updates but doesnt analyze in the SIEM.

B . Parser:Processes logs but doesnt provide comparison insights.

C . Filter query:Excludes matches, opposite of enrichment.

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

QUESTION 152

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

OnlyHOST002is 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

Understanding the Security Event:

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

This indicatesunauthorized access, which could bea sign of lateral movement or network infection. This is ared flagfor potential malware, unauthorized software, or a compromised host.

Unusual network traffic patternsare often an indicator of acompromised system. VM002 should not be communicating externally, but it is.

This suggests a possiblebreach or malware infectionattempting to communicate with a commandand-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 isfrom VM002.

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

CompTIASecurityX 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

QUESTION 153

A company recentlyexperienced aransomware attack. Although the company performssystems and data backupon a schedule that aligns with itsRPO (Recovery Point Objective) requirements, thebackup administratorcould not recovercritical systems and datafrom its offline backups to meet the RPO. Eventually, the systems and data were restored with information that wassix 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

Understanding the Ransomware Issue:

The key issue here is thatbackups were not recoverable within the required RPO timeframe. This means the organizationdid not properly testitsbackup 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 functionaland can meetbusiness continuity needs. Frequent DR testingallows organizations to identify and fixgaps in recovery strategies.

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

B (Reverting to manual business processes):While amanual continuity planis good for resilience, it doesnot resolve the backup and recovery failure.

D (Tabletop exercise & RACI matrix):Atabletop exerciseis a planning activity, butit 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

QUESTION 154

A compliance officer isfacilitating abusiness impact analysis (BIA)and wantsbusiness unit leadersto collect meaningful data. Several business unit leaders want more information about the types of data the officer needs.

Which of the following data types would be the most beneficial for the compliance officer?(Select two)

A. Inventory details

B. Applicable contract obligations

C. Costs associated with downtime

D. Network diagrams

E. Contingency plans

F. Critical processes

Answer: B,C,F

Understanding Business Impact Analysis (BIA):

ABIA assesses the effects of disruptionsto an organization's operations.

It helpsprioritize resourcesbased on the potential impact ofdowntime, compliance issues, and critical processes.

Why Options B, C, and F are Correct:

B (Applicable contract obligations)â†' Many companies havelegal and compliance obligationsregarding downtime, availability, and SLAs. This information helps determine whatrisk levelsare acceptable.

C (Costs associated with downtime)â†' BIA quantifies the financial impact of system failures. Knowinglost revenue, regulatory fines, and recovery costshelps in planning.

F (Critical processes)â†' Identifyingcore business processesallows an organization toprioritize recoveryeffortsandmaintain operational continuity.

A (Inventory details)â†' While useful for asset management, it doesnot directly impact business continuity planning.

D (Network diagrams)â†' These help in security architecture but arenot directly related to the financial/business impact analysis.

E (Contingency plans)â†' BIA isperformed before contingency planningto identifywhat needs protection.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide:Business Impact Analysis (BIA) & Risk Management NIST SP 800-34:Business Continuity & Contingency Planning

QUESTION 155

A companysSIEMis designed to associate the companysasset 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	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 thefollowing should asecurity engineer investigate firstas part of alog audit?

A. Anendpointthat is not submitting any logs

B. Potential activity indicating an attackermoving laterally in the network

C. Amisconfigured syslog servercreating false negatives

Answer: D. Unauthorized usage attempts of the administrator account D

Understanding the Security Event:

Administrator accounts are highly privilegedand require strict monitoring.

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

The fact thatnone of the admin login attempts were successfulsuggestssomeone was trying to guess

Why Option D isCorrect:

Failed logins for administrator accounts are a critical security concern.

If an attacker gains access, they couldescalate privileges and compromise the network. Investigatingunauthorized admin login attemptsshould be thetop priorityin a log audit. Why Other Options Are Incorrect:

A (Endpoint not submitting logs):While this is concerning, it does not indicate anactive 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 thefailed admin loginsare real. Reference:

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

QUESTION 156

During a recentsecurity event, access from thenon-production environment to the production environmentenabledunauthorized usersto:

Installunapproved software Makeunplanned configuration changes

During theinvestigation, the following findings were identified:

Several new users were added in bulkby theIAM team Additionalfirewalls and routerswere recently added

Vulnerability assessmentshave been disabled formore than 30 days Theapplication allow listhas not been modified intwo weeks

Logs were unavailablefor various types of traffic Endpoints have not been patchedinover ten days

Which of the following actions would most likely need to be taken toensure proper monitoring?(Select two)

A. Disable bulk user creationsby the IAM team

B. Extend log retention for all security and network devices to180 daysfor all traffic

C. Review the application allow listdaily

D. Routinely update allendpoints and network devicesas soon as new patches/hot fixes are available

E. Ensure allnetwork and security devicesare sending relevant data to theSIEM

Answer: F. Configure firewall rules toonly allow production-to-non-productiontraffic A,D,E

Understanding the Security Event:

Unauthorized usersgained access from non-production to production. IAM policies were weak, allowingbulk user creation.

Why Options A, D, and E areCorrect:

A (Disable bulk user creation by IAM team)â†' Prevents unauthorized mass user account creation, which could beexploited by attackers.

D (Routine updates for endpoints & network devices)â†' Patch management ensuresvulnerabilities are not left open for attackers.

E (Ensure all security/network devices send logs to SIEM)â†' Helps withreal-time monitoring and detection of unauthorized activities.

Why Other Options Are Incorrect:

B (180-day log retention)â†' While log retention is good,real-time monitoring is the priority.

C (Review application allow list daily)â†' Reviewing itdaily is impractical. Regular audits are better. F (Restrict production-to-non-production traffic)â†' The issue isunauthorized access, not traffic routing.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide:IAM, Patch Management & SIEM Logging Best Practices

NIST 800-53 (AC-2, AU-12):Audit Logging & Access Control

QUESTION 157

An organization hires a security consultant to establish a SOC that includes athreat-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

Answer: E. A current inventory of cloud resources and SaaS products in use C

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 riskinducing.

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

Reference:CompTIA SecurityX CAS-005Official Study Guide, Chapter 3: "Threat Modeling and Security Assessments," Section 3.2: "Understanding Data Flow Diagrams."

QUESTION 158

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

Answer: E. Software composition analysis A

Regression testing is a software testingpractice 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 complexsystems where multiple components interact. Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 8: "Software Development Security," Section 8.3: "Testing and Validation Processes."

==========

QUESTION 159

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?

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: A

A risk register is atool 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.

Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 6: "Risk Management," Section

6.4: "Risk Register and Risk Ownership."

==========

QUESTION 160

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

Answer: D. Protecting privacy while supporting portability D

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.

Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 11: "Data Security," Section

11.3: "Data Encryption and Protection Mechanisms."

QUESTION 161

A company was recently infected by malware. During the root cause analysis, the company determined that several users were installing their own applications. To prevent further

A. Signing

B. Access control

C. HIPS

D. Permit listing

Answer: D

To prevent unauthorized applications from running, the company needs a mechanism to explicitly define and enforce which applications are allowed to execute. "Permit listing" (often referred to as "whitelisting" in security contexts) is the most effective solution here. It involves creating a list of approved applications, and only those on the list are permitted to run, blocking all others by default. This directly addresses the root cause”users installing unapproved software”by restricting execution to only authorized programs.

Option A (Signing):Code signing ensures the authenticity and integrity of software by verifying it comes from a trusted source and hasnt been tampered with. While useful, it doesnt inherently prevent unauthorized applications from running unless combined with a policy like whitelisting. Option B (Access control):Access control governs who can access systems or resources but doesnt specifically restrict which applications can execute. Its too broad for this scenario.

Option C (HIPS):A Host-based Intrusion Prevention System (HIPS) can detect and block malicious behavior, but its reactive and relies on signatures or heuristics, not a proactive allow-only approach. Option D (Permit listing):This is the best fit, as it proactively enforces a policy where only explicitly authorized applications can run, preventing malware introduced by unauthorized software.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture “ Application Security Controls.

QUESTION 162

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice. Which of the following should the organization consider first to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.

B. Hire additional on-call staff to be deployed if an event occurs.

C. Design an appropriate warm site for business continuity.

D. Identify critical business processes and determine associated software and hardware requirements.

Answer: D

For a disaster recovery (DR) plan requiring immediate data availability, the first step is understanding what needs to be protected and recovered. Identifying critical business processes and their

associated software and hardware requirements establishes the foundation for the DR plan. This ensures that backups and recovery mechanisms align with business priorities, meeting the "moment's notice" requirement.

Option A:A change management plan is important for system consistency but doesnt directly address immediate data availability in a DR context.

Option B:Hiring staff supports execution but doesnt define what needs to be recovered or how. Its a later step.

Option C:A warm site (a partially operational backup site) is a good DR solution, but designing it comes after identifying critical processes and resources.

Option D:This is the first step in any DR planning process”knowing whats critical ensures the plan meets availability goals efficiently.

Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations " Disaster Recovery and Business Continuity Planning.

QUESTION 163

A technician is reviewing the logs and notices a large number of files were transferred to remote

sites over the course of three months. This activity then stopped. The files were transferred via TLSprotected HTTP sessions from systems that do not normally send traffic to those sites. The technician

will define this threat as:

A. A decrypting RSA using an obsolete and weakened encryption attack.

B. A zero-day attack.

C. An advanced persistent threat.

D. An on-path attack.

Answer: C

The scenario describes a prolonged, stealthy operation where files were exfiltrated over three

months via secure channels (TLS-protected HTTP) from unexpected systems, then ceased. This aligns with anAdvanced Persistent Threat (APT), characterized by long-term, targeted attacks aimed at data theft or surveillance, often using sophisticated methods to remain undetected.

Option A:Decrypting RSA with weak encryption implies a cryptographic attack, but TLS suggests modern encryption was used, and theres no evidence of decryption here.

Option B:A zero-day attack exploits unknown vulnerabilities, but the duration and cessation suggest a planned operation, not a single exploit.

Option C:APT fits perfectly"slow, persistent exfiltration fromunusual systems indicates a coordinated, stealthy threat actor.

Option D:An on-path (man-in-the-middle) attack intercepts traffic, but theres no indication of

Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management “ Threat Identification and Analysis.

QUESTION 164

Due to locality and budget constraints, an organizations satellite office has a lower bandwidth allocation than other offices. As a result, the local securityinfrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal

and external resources while not sacrificing threat visibility. Which of the following would be the best option to implement?

A. Distributed connection allocation

B. Local caching

C. Content delivery network

Answer: D. SD-WAN vertical heterogeneity B

The goal is to optimize bandwidth, increase speed, and maintain threat visibility in a low-bandwidth satellite office.Local cachingstores frequently accessed data locally, reducing bandwidth usage by minimizing repeated requests to external or internal resources. It speeds up access and doesnt inherently reduce security visibility if paired with monitoring tools.

Option A:Distributed connection allocation might balance traffic but doesnt directly reduce bandwidth usage or speed up access.

Option B:Local caching is ideal”reduces bandwidth, improves performance, and maintains visibility with proper security controls.

Option C:A CDN is great for external content delivery but less relevant for internal resources and doesnt inherently address threat visibility.

Option D:SD-WAN improves WAN performance, but "vertical heterogeneity" is vague and not a standard term; its less tailored to this scenario than caching.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture “ Network Optimization and Security.

QUESTION 165

Which of the following supports the process of collecting a large pool of behavioral observations to inform decision-making?

A. Linear regression

B. Distributed consensus

C. Big Data

D. Machine learning

Answer: C

Collecting a large pool of behavioral observations requires handling vast datasets, which is the domain ofBig Data. Big Data technologies enable the storage, processing, and analysis of large-scale data (e.g., user behavior logs) to inform decisions, a key capability in security analytics.

Option A:Linear regression is a statistical method for modeling relationships, not collecting data. Option B:Distributed consensus relates to agreement in distributed systems (e.g., blockchain), not data collection.

Option C:Big Data directly supports collecting and analyzing large datasets for insights, fitting the question perfectly.

Option D:Machine learning uses data to train models but relies on data being collected first, often via Big Data.

Reference:CompTIA SecurityX CAS-005 Domain 3: Research, Development, and Collaboration “ Data Analytics for Security.

QUESTION 166

A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Select three).

A. Temporal

B. Availability

C. Integrity

D. Confidentiality

E. Base

F. Environmental

G. Impact

Answer: H. Attack vector A,E,F

The Common Vulnerability Scoring System (CVSS) v3.1 uses three metric groups to calculate overall scores:Base,Temporal, andEnvironmental.

Base (E):Mandatory metrics assessing exploitability (e.g., attack vector) and impact (confidentiality, integrity, availability).

Temporal (A):Optional metrics reflecting the current state of the vulnerability (e.g., exploit availability, remediation level).

Environmental (F):Optional metrics tailoring the score to the organizations context (e.g., security requirements).

G (Impact):A categorywithin Base, not a group.

H (Attack vector):A single Base metric, not a group.

Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management " Vulnerability Assessment and Prioritization.

QUESTION 167

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

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 solutions effectiveness, ensuring accurate metrics for decision-making without production impact.

Option A:Testing all solutions simultaneously muddies the results"metrics wont 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.

Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations " Incident Response and Testing.

QUESTION 168

An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about

A. Ladder logic

B. Rust

C. C

D. Python

Answer: E. Java A

Programmable Logic Controllers (PLCs) in Operational Technology (OT) environments commonly useLadder Logic, a graphical programming language resembling electrical relay logic diagrams. Its the most relevant for PLCs due to its widespread use in industrial automation.

Option A:Ladder Logic is the standard for PLC programming, making it the best choice. Option B:Rust is modern and secure but not typically used for PLCs.

Option C:C is used in some embedded systems but less common for PLCs. Option D:Python is versatile but not native to PLC programming.

Option E:Java is rare in PLC contexts.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture " OT Security and Secure Coding.

QUESTION 169

A security engineer is implementing a code signing requirement for all code developed by the organization. Currently, the PKI only generates website certificates. Which of the following steps should the engineer perform first?

A. Add a new template on the internal CA with the correct attributes.

B. Generate a wildcard certificate for the internal domain.

C. Recalculate a public/private key pair for the root CA.

D. Implement a SAN for all internal web applications.

Answer: A

To enable code signing with an existing PKI, the first step is to configure the Certificate Authority (CA) to issue code signing certificates. Adding a new template with attributes specific to code signing

(e.g., key usage for signing) allows the CA to support this requirement without disrupting existing operations.

Option A:Correct”templates define certificate types; this isthe foundational step. Option B:Wildcard certificates are for domains, not code signing.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture " PKI Implementation.

QUESTION 170

Which of the following are risks associated with vendor lock-in? (Select two).

A. The client can seamlessly move data.

B. The vendor canchange product offerings.

C. The client receives a sufficient level of service.

D. The client experiences decreased quality of service.

E. The client can leverage a multicloud approach.

F. The client experiences increased interoperability.

Answer: B,D

Vendor lock-in occurs when a client is overly dependent on a vendor, limiting flexibility. Risks include: Option B:Vendors changing offerings (e.g., features, pricing) can disrupt the client, a key lock-in risk.

Option D:Decreased quality of service may result from reliance on a single vendor without alternatives.

Option A:Seamless data movement is a benefit, not a risk. Option C:Sufficient service is neutral or positive, not a risk. Option E:Multicloud is hindered by lock-in, not a risk of it.

Option F:Increased interoperability contradicts lock-ins limitations.

Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management " Vendor Risk Assessment.

QUESTION 171

An auditor is reviewing the logs from a web application to determine the source of an incident. The web application architecture includes an internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

Web server logs:

192.168.1.10 - - [24/Oct0 11:24:34 +05:00] "GET /bin/bash" HTTP.1" 200 453 Safari.36

192.168.1.10 - - [24/Oct0 11:24:35 +05:00] "GET / HTTP.1" 200 453 Safari.36

Application server logs:

24/Oct0 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB

24/Oct0 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing Database server logs:

24/Oct0 11:24:34 +05:00 [Warning] 'option read_buffer_size1 unassigned value 0 adjusted to

24/Oct0 11:24:35 +05:00 [Warning] CA certificate ca.pem is self-signed.

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the X-Forwarded-For header at the load balancer.

B. Install a software-based HIDS on the application servers.

C. Install a certificate signed by a trusted CA.

D. Use stored procedures on the database server.

E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Answer: A

The issue is tracing the original source of requests in a tiered architecture with a load balancer. The web server logs show internal IPs (192.168.1.10), not the external client IPs, because the load balancer forwards requests without preserving the source. Enabling theX-Forwarded-Forheader on the load balancer adds the clients original IP to the HTTP request headers, allowing downstream servers to log it. This ensures traceability without altering the architecture significantly.

Option A:Correct”X-Forwarded-For is the standard solution for preserving client IPs through load balancers.

Option B:A Host-based Intrusion Detection System (HIDS) detects anomalies but doesnt address IP traceability.

Option C:A trusted CA certificate fixes the self-signed warning but is unrelated to source tracking. Option D:Stored procedures improve database security but dont help with IP logging.

Option E:Storing $_SERVER['REMOTE_ADDR'] captures the loadbalancers IP, not the clients, unless X-Forwarded-For is enabled.

Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations “ Log Analysis and Incident Investigation.

QUESTION 172

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of the impact. Which of the following should the organization perform next?

A. Assess the residual risk.

B. Update the organization's threat model.

C. Move to the next risk in the register.

D. Recalculate the magnitude of the impact.

Answer: A

After applying mitigations that reduce the likelihood of a risks impact, the next step is toassess the residual risk"the risk that remains after controls are implemented. This ensures the organization understands if the mitigation is sufficient or if further action is needed, aligning with risk management best practices.

Option A:Correct"residual risk assessment is the logical next step to evaluate the effectiveness of mitigations.

Option B:Updating the threat model might follow but isnt immediate; residual risk comes first. Option C:Moving to the next risk skips evaluating the current mitigations success.

Option D:Recalculating impact magnitude is part of residual risk assessment but isnt the full process. Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management " Risk Mitigation and Residual Risk Analysis.

QUESTION 173

A security analyst is reviewing the following vulnerability assessment report:

192.168.1.5, Host = Server1, CVSS 7.5, Web Server, Remotely Executable = Yes, Exploit = Yes 205.1.3.5, Host = Server2, CVSS 6.5, Bind Server, Remotely Executable = Yes, Exploit = POC 207.1.5.7, Host = Server3, CVSS 5.5, Email Server, Remotely Executable = Yes, Exploit = Yes 192.168.1.6, Host = Server4, CVSS 9.8, Domain Controller, Remotely Executable = Yes, Exploit = Yes Which of the following should be patched first to minimize attacks against internet-facing hosts?

A. Server1

B. Server2

C. Server3

Answer: D. Server4 B

The question focuses oninternet-facing hosts, implying external exposure. CVSS scores, remote executability, and exploitavailability guide prioritization. Server2 (205.1.3.5, CVSS 6.5, Bind Server) has a public IP, suggesting its internet-facing, unlike Server1 and Server4 (192.168.x.x, private IPs). Server3 (207.1.5.7, CVSS 5.5) is also public but has a lower score and risk compared to Server2s proof-of-concept (POC) exploit. Server2s Bind Server (DNS) role is critical and commonly targeted, making it the priority.

Option A:Server1 (CVSS 7.5) is private, not internet-facing.

Option B:Server2 (CVSS 6.5) is internet-facing with an exploit POC, warranting immediate patching. Option C:Server3 (CVSS 5.5) is internet-facing but less severe.

Option D:Server4 (CVSS 9.8) is critical but private, not internet-facing.

Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management " Vulnerability Prioritization.

PKI can be used to support security requirements in the change management process. Which of the following capabilities does PKI provide for messages?

A. Non-repudiation

B. Confidentiality

C. Delivery receipts

Answer: D. Attestation A

Public Key Infrastructure (PKI) supports change management by securing messages (e.g., approvals, updates).Non-repudiation, provided via digital signatures, ensures a sender cannot deny sending a message, critical for auditability in change processes.

Option A:Correct”PKIs digital signatures ensure non-repudiation.

Option B:Confidentiality (via encryption) is a PKI feature but less tied to change managements focus on accountability.

Option C:Delivery receipts are not aPKI function; theyre protocol-specific (e.g., SMTP). Option D:Attestation relates to verifying attributes, not a direct PKI message capability.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture “ PKI and Secure Processes.

QUESTION 175

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack. Which of the following is the next step of the incident response plan?

A. Remediation

B. Containment

C. Response

D. Recovery

Answer: B

Incident response follows a standard process (e.g., NIST 800-61): Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned. After identifying the attack (file and origin), the next step isContainment”limiting the spread or impact (e.g., isolating systems) before remediation or recovery.

Option A:Remediation (fixing the root cause) follows containment.

Option B:Correct”containment prevents further damage post-identification.

Option D:Recovery (restoring systems) comes after containment and eradication. Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations “ Incident Response Lifecycle.

QUESTION 176

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 analysts findings and a potential mitigation technique?

A. The findingsindicate 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: C

The error message reveals sensitive details (hostnames, database names, table names), constitutinginformation disclosure. This aids attackers in reconnaissance. Mitigation involves modifying the application to display generic error messages (e.g., œAn 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 doesnt address disclosure.

Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture “ Secure Application Design and Error Handling.

QUESTION 177

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

C. Ansible

D. PowerShell

Answer: C

Automating compliance in cloudenvironments requires a tool that can enforce configurations, manage infrastructure as code, and align with industry standards (e.g., NIST, ISO). Lets evaluate:

A . Jenkins:A CI/CD tool for automating software builds and deployments. Its 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.

QUESTION 178

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 administrators 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 administrators named accounts.

Answer: B

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. Lets analyze:

A . Token theft detection with lockouts:Useful for detecting stolen SSO tokens, but its reactive and

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-005s focus on adaptive security.

C . Decentralize accounts:This removes SSO, increasing complexity and weakening MFA enforcement, which isnt practical or secure.

Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, emphasizing context-aware authentication for SSO environments.

QUESTION 179

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: A

Integrating IDS, firewall, and DLP to reduce response time requires orchestration and automation. Lets evaluate:

A . SOAR(Security Orchestration, Automation, and Response):SOAR integrates security tools, automates workflows, and speeds up incident response. Its the best fit for this scenario, as CAS-005 highlights SOAR for operational efficiency.

B . CWPP (CloudWorkload 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.

Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, focusing on SOAR for tool integration.

QUESTION 180

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

Answer: D. Centralized logging B

Managing telemetry and differentiating it by office requires a way to categorize data. Lets evaluate:

A . Sensor placement:Useful for data collection but doesnt inherently differentiate by office.

B . Data labeling:Assigns metadata (e.g., office location) to telemetry, enabling differentiation. This aligns with CAS-005s focus on data management for security operations.

C . Continuous monitoring:Ensures ongoing data collection but doesnt address differentiation. Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, emphasizing telemetry management.

QUESTION 181

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

The requirements demand detailed asset tracking and inventory management. Lets 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 doesnt 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.

QUESTION 182

A senior security engineer flags the following log file snippet as having likely facilitated an attackers lateral movement in a recent breach:

qry_source: 19.27.214.22 TCP

| 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

C. Implementing DNS masking on internal servers

Answer: D. Permitting only clients from internal networks to query DNS A

The log shows an AXFR (zone transfer) query, which exposed internal DNS records, aiding lateral movement. Lets 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-005s security operations focus.

B . Restricting to UDP:AXFR uses TCP, so this wouldnt stop it.

C . DNSmasking:Obscures records but isnt a standard term for this fix.

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

QUESTION 183

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

C. Rotating KRBTGT password

Answer: D. Resetting the local domain C

The attacker gained domain control by collecting the KRBTGT hash (used for Kerberos tickets). Lets 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-005s focus on identity security.

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

QUESTION 184

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

Determining if attacks are from the same actor requires unique attribution. Lets analyze:

A . Code stylometry:Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005s threat intelligence focus.

B . Common IOCs:Indicates similar attacks but not necessarily the same actor.

C . IOCextractions:Similar to B, lacks specificity for attribution.

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

QUESTION 185

An external threat actor attacks public infrastructure providers. In response to the attack and during follow-up activities, various providers share information obtained during response efforts. After the attack, energy sector companies share their status and response data:

Company SIEM UEBA DLP

ISAC Member TIP Integration Time to Detect Time to Respond 1

Yes No Yes Yes Yes

10 minutes

20 minutes

2

Yes Yes Yes Yes No

20 minutes

40 minutes

3

Yes Yes No No Yes

12 minutes

24 minutes

Which of thefollowing is the most important issue to address to defend against future attacks?

A. Failure to implement a UEBA system

B. Failure to implement a DLP system

C. Failure to join the industry ISAC

Answer: D. Failure to integrate with the TIP C

(12 minutes) and response (24 minutes) times, despite having UEBA and TIP integration. Company 2, which lacks TIP integration but is an ISAC member, has the slowest times (20 minutes to detect, 40 minutes to respond). This suggests that ISAC membership correlates with faster detection and response, likely due to access to shared threat intelligence.

According to the CompTIA SecurityX CAS-005 objectives (Domain 2: Security Operations, 2.2),

Information Sharing and Analysis Centers (ISACs) are critical for enabling organizations to share realtimethreat intelligence within their industry. ISACs provide access to actionable intelligence, best

practices, and coordinated response strategies, which are essential for defending against sophisticated attacks targeting critical infrastructure like the energy sector. The lack of ISAC membership (Company 3) limits access to this intelligence, hindering proactive defense and

response capabilities. While UEBA, DLP, and TIP integration are valuable, they are more focused on internal monitoring, data protection,and individual threat intelligence feeds, respectively, and do not provide the same industry-wide collaboration as an ISAC.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 2: Security Operations, Section 2.2: "Explain the importance of threat intelligence sharing and collaboration, including ISACs."

CAS-005 Exam Objectives, 2.2: "Analyze the impact of information sharing on incident response efficiency."

QUESTION 186

Which of the following best describes the challengesassociated with widespread adoption of homomorphic encryption techniques?

A. Incomplete mathematical primitives

B. No use cases to drive adoption

C. Quantum computers not yet capable

Answer: D. Insufficient coprocessor support D

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, preserving confidentiality. However, its adoption faces significant challenges due to performance overhead. According to the CompTIA SecurityX CAS-005 study materials (Domain 3: Cybersecurity Technology, 3.3), homomorphic encryption requires substantial computational resources, which standard processors struggle to provide efficiently. Specialized hardware, such as coprocessors (e.g., GPUs or TPUs), is oftenneeded to handle the complex mathematical operations

Option A (Incomplete mathematical primitives):While early homomorphic encryption schemes had limitations, modern schemes (e.g., CKKS, BFV) have mature mathematical foundations, making this less of a challenge today.

Option B (No use cases):Use cases exist, such as secure cloud computing and privacy-preserving data analytics, so this is not accurate.

Option C (Quantum computers):Homomorphic encryption is not dependent on quantum computing, and quantum computers are unrelated to its current challenges.

Option D (Insufficient coprocessor support):This is the most accurate, as performance bottlenecks require specialized hardware that is not yet widely available or integrated.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.3: "Evaluate emerging cryptographic technologies, including homomorphic encryption challenges."

CAS-005 Exam Objectives, 3.3: "Analyze barriers to adopting advanced encryption techniques."

QUESTION 187

Which of the following best describes the reason a network architect would enable forward secrecy on all VPN tunnels?

A. This process is a requirement to enable hardware-accelerated cryptography.

B. This process reduces the success of attackers performing cryptanalysis.

C. The business requirements state that confidentiality is a critical success factor.

D. Modern cryptographic protocols list this process as a prerequisite for use.

Answer: B

Forward secrecy (also known as perfect forward secrecy, PFS) ensures that session keys used in a VPN tunnel are ephemeral, meaning that even if an attacker compromises a long-term private key, past sessions cannot be decrypted. According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.1), enabling forward secrecy on VPN tunnels reduces the risk of cryptanalysis by ensuring that each sessions encryption key is unique and not derived from a single compromised key. This directly mitigates the impact of attacks like key theft or future decryption attempts.

Option A:Forward secrecy is not required for hardware-accelerated cryptography, which depends on processor capabilities, not key management.

Option C:While confidentiality is important, this is too vague and does not specifically explain why forward secrecy is chosen.

Option D:Modern protocols (e.g., TLS 1.3, IPsec with ECDHE) support forward secrecy but donot mandate it as a prerequisite for use.

Option B:This is the most precise, as forward secrecy directly reduces the success of cryptanalysis by

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.1: "Explain cryptographic techniques, including perfect forward secrecy."

CAS-005 Exam Objectives, 3.1: "Evaluate the impact of cryptographic configurations on security."

QUESTION 188

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

Answer: D. Updating security mobile reporting policies and monitoring data breaches A

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 protectingsensitive data on endpoints."

QUESTION 189

A global companys Chief Financial Officer (CFO) receives a phone call from someone claiming to be the Chief Executive Officer (CEO). The caller claims to be stranded and in desperate need of money. The CFO is suspicious, but the callers voice sounds similar to the CEOs. Which of the following best

A. Smishing

B. Deepfake

C. Automated exploit generation

D. Spear phishing

Answer: B

This scenario describes an attack where the attacker mimics the CEOs voice to deceive the CFO,

likely using AI-generated audio. According to the CompTIA SecurityX CAS-005 study guide (Domain 1:

Security Strategy and Risk Management, 1.2), a deepfake attack involves using artificial intelligence to create realistic but fake audio, video, or other media to impersonate someone. In this case, the voice similarity suggests a deepfake audio attack, which is a targeted social engineering tactic.

Option A:Smishing involves SMS-based phishing, not voicecalls.

Option C:Automated exploit generation refers to creating software exploits, not impersonation. Option D:Spear phishing targets specific individuals but typically via email, not voice-based impersonation.

Option B:Deepfake is the most accurate, as it describes AI-driven impersonation of the CEOs voice. Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 1: Security Strategy and Risk Management,

Section 1.2: "Identify advanced social engineering attacks, including deepfakes." CAS-005 Exam Objectives, 1.2: "Analyze the impact of AI-based attacks on security."

QUESTION 190

A cloud engineer wants to configure mail security protocols to support email authenticity and enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured to achieve these requirements? (Select two).

A. DMARC

B. DKIM

C. TLS

D. SPF

E. DNSSEC

F. MX

Answer: A,B

To support email authenticity and enable analysis by a third-party platform, the protocols must verify

DMARC (Domain-based Message Authentication, Reporting, and Conformance):DMARC builds on SPF and DKIM to enforce policies for email authenticity and provides reporting mechanisms to share authentication results with third parties for analysis.

DKIM (DomainKeys Identified Mail):DKIM adds a cryptographic signature to emails, allowing recipients to verify the senders domain and ensure the emails integrity.

These two protocols are essential for authenticity and reporting.

Option C (TLS):TLS ensures encryption during transmission but does not address authenticity or reporting.

Option D (SPF):SPF verifies sender IP addresses but lacks reporting capabilities without DMARC. Option E (DNSSEC):DNSSEC secures DNS queries but is not specific to email authenticity.

Option F (MX):MX records define mail servers, not authenticity or reporting. Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.2: "Configure email security protocols, including DMARC and DKIM."

CAS-005 Exam Objectives, 3.2: "Implement technologies for email security and authenticity."

QUESTION 191

A company is preparing to move a new version of a web application to production. No issues were reported during security scanning or quality assurance in the CI/CD pipeline. Which of the following actions should thecompany take next?

A. Merge the test branch to the main branch

B. Perform threat modeling on the production application

C. Conduct unit testing on the submitted code

Answer: D. Perform a peer review on the test branch A

The question states that security scanning and quality assurance (QA) in the CI/CD pipeline have been completed with no issues, indicating that the code in the test branch is ready for production.

According to the CompTIA SecurityX CAS-005 study guide (Domain 2: Security Operations, 2.3), in a secure CI/CD pipeline, once code passes automated security scans, QA, and other checks (e.g., unit testing, peer reviews), the next step is to merge the tested branch into the main branch for

deployment to production.

Option B:Threat modeling is typically performed earlier, during design or development, not after passing CI/CD checks.

Option C:Unit testing is part of the CI/CD pipeline and should already be completed.

Option D:Peer reviews are conducted before or during the test phase, not after QAand security scans are clear.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 2: Security Operations, Section 2.3: "Manage secure software development lifecycles, including CI/CD pipelines."

CAS-005 Exam Objectives, 2.3: "Analyze secure deployment processes in CI/CD environments."

QUESTION 192

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

Answer: D. To leverage asymmetric encryption for large amounts of data A

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., Shors 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 PQCs 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."

QUESTION 193

A security team determines that the most significant risks within the pipeline are: Unauthorized code changes

The current inability to perform independent verification of software modules Which of the following best addresses these concerns?

B. Digital signatures

C. Non-repudiation

Answer: D. Lightweight cryptography A

Unauthorized code changesand lack ofindependent verificationare directly mitigated bycode signing, which ensures that code is from a trusted source and has not been altered.

While digital signatures are part of code signing, the broader practice of code signing encompasses signature management, version integrity, and trusted sources.

Lightweight cryptography is irrelevant in this context; it's more about efficiency in constrained devices.

Non-repudiation is a benefit of digital signatures but doesn't directly solve the verification/integrity concerns alone.

FromCAS-005 Guide, Domain 4: Security Architecture, Tools, and Technologies:

œCode signing ensures that the code has not been tampered with and originates from a trusted developer.

Reference:CAS-005 Official Study Guide, Chapter 10: Secure Development Operations, pg. 201“204

QUESTION 194

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:

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

Theregulated lab environment (Yes)shares the same VLAN (10.2.0.0) withusers, creatingzone traversalrisk from unregulated zones to sensitive datanetworks.

This allows pivoting and lateral movement from non-regulated user devices into regulated lab environments ” a classiczone boundary violation.

Zone traversal should be mitigated with segmentation and firewall enforcement. FromCAS-005, Domain 2: Risk Management and Mitigation Strategies:

œZone 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

An organization plans to deploy new software. The project manager compiles a list of roles that will be involved in different phases of the deployment life cycle. Which of the following should the project manager use to track these roles?

A. CMDB

B. Recall tree

C. ITIL

Answer: D. RACI matrix D

RACI matrix(Responsible, Accountable, Consulted, Informed) is used for role mapping across the project lifecycle.

CMDB is a configuration inventory; ITIL is a framework. Recall trees are for disaster recovery/business continuity.

FromCAS-005, Domain 1: Security Governance and Compliance:

œThe RACI matrix is essential in role assignment and accountability for software development and operational processes.

Reference:CAS-005 Official Guide, Chapter 3: Governance Frameworks, pg. 78“79

QUESTION 196

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

OpenSSH vulnerabilityispublic facingand has acritical CVSS of 9.2. Exploitable SSH services can lead to direct server compromise.

Although Apache has a higher score, it's internal. FromCAS-005, Domain 3: Vulnerability Management:

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

QUESTION 197

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. Configuring the CPU's NX bit

B. Enabling a host firewall

C. Enabling an edge firewall

D. Enforcing all systems to use UEFI

Answer: E. Enabling ASLR on the Active Directory server B

The malware uses TCP 4444 to move laterally between systems. A host-based firewall can block unauthorized communication ports (like TCP 4444) on each workstation, preventing malware from establishing connections and spreading. Configuring the CPU's NX bit and enabling ASLR primarily help in mitigating memory-based exploits, not in stopping lateral movement. Enabling UEFI ensures boot integrity but does not mitigate active lateral communication. An edge firewall would protect

the network perimeter, not internal workstation-to-workstation communication. Reference:CompTIA SecurityX CAS-005, Domain 2.0: Implement host-based security solutions, including host-based firewalls to mitigate threats.

QUESTION 198

Company A acquired Company B. During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program. Which of the following risk-handling techniques was used?

B. Avoid

C. Transfer

D. Mitigate

Answer: D

Risk mitigation involves taking actions to reduce either the likelihood or impact of a threat. By implementing a firewall between the two environments, Company A is minimizing the risk of threats from Company B impacting its own systems. Accepting the risk would involve taking no action, avoiding it would mean terminating activities with Company B, and transferring would involve outsourcing the risk, none of which occurred here.

Reference:CompTIA SecurityX CAS-005, Domain 1.0: Apply appropriate risk response techniques to identified risks.

QUESTION 199

An organization recently implemented a purchasing freeze that has impacted endpoint life-cycle management efforts. Which of the following should a security manager do to reduce risk without replacing the endpoints?

A. Remove unneeded services

B. Deploy EDR

C. Dispose of end-of-support devices

Answer: D. Reimage the system A

Removing unnecessary services from existing endpoints reduces the attack surface by minimizing the number of potential vulnerabilities attackers could exploit. This is a cost-effective method to harden devices without requiring new purchases, aligning perfectly with a purchasing freeze. Deploying new EDR solutions or disposing of devices would likely conflict with the resource freeze, and reimaging systems does not address minimizing services proactively.

Reference:CompTIA SecurityX CAS-005, Domain 3.0: Implement endpoint security controls and hardening techniques.

QUESTION 200

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?

B. Legal issues

C. Chain of custody

D. Order of volatility

E. Key exchange

Answer: C

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.

QUESTION 201

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

Answer: D. Request that the affected servers be restored immediately B

The immediate action after discovering ransomware is toisolate the affected serversto 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.

QUESTION 202

The device event logs sourced from MDM software are as follows:

Device | Date/Time | Location | Event | Description

ANDROID_102 | 01JAN21 0255 | 38.9072N, 77.0369W | PUSH | APPLICATION 1220 INSTALL QUEUED ANDROID_102 | 01JAN21 0301 | 38.9072N, 77.0369W | INVENTORY | APPLICATION 1220 ADDED ANDROID_1022 | 01JAN21 0701 | 39.0067N, 77.4291W | CHECK-IN | NORMAL

ANDROID_1022 | 01JAN21 0701 | 25.2854N, 51.5310E | CHECK-IN | NORMAL ANDROID_1022 | 01JAN21 0900 | 39.0067N, 77.4291W | CHECK-IN | NORMAL

ANDROID_1022 | 01JAN21 1030 | 39.0067N, 77.4291W | STATUS | LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would best address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220

B. Resource leak; recover the device for analysis and clean up the local storage

C. Impossible travel; disable the device's account and access while investigating

Answer: D. Falsified status reporting; remotely wipe the device C

The logs show the device checking in from two distant locations (USA and Qatar) at nearly the same time, which indicatesimpossible travel" a strong indicator that either the device has been cloned, compromised, or credentials stolen. The best immediate action is todisable the device's account and accessto prevent potential misuse while an investigation is

conducted. Malicious application installation or resource issues are possible but secondary concerns here compared to account compromise.

Reference:CompTIA SecurityX CAS-005, Domain 2.0: Detect and analyze anomalous behavior in mobility solutions and respond appropriately.

QUESTION 203

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

Answer: unauthenticated users C

Homomorphic encryptionallows 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.

QUESTION 204

A security architect is investigating instances of employees who had their phones stolen in public places through seemingly targeted attacks. Devices are able to access company resources such as email and internal documentation, some of which can persist in application storage. Which of the following would best protect the company from information exposure? (Select two).

A. Implement a remote wipe procedure if the phone does not check in for a period of time

B. Enforce biometric access control with configured timeouts

C. Set up geofencing for corporate applications where the phone must be near an office

D. Use application control to restrict the applications that can be installed

E. Leverage an MDM solution to prevent the side loading of mobile applications

Answer: F. Enable device certificates that will be used for access to company resources A,B

To protect company information on stolen mobile devices, implementingremote wipe proceduresensures data can be erased if a device is suspected lost or stolen.Biometric access controlwith enforced timeouts further secures the device, requiring biometric authentication periodically, thus limiting unauthorized access even if the device is stolen. Geofencing and certificates provide additional security layers but are less immediate protections against information exposure after theft. Application control and side-loading prevention are important for malware threats but less so for stolen device scenarios.

Reference:CompTIA SecurityX CAS-005, Domain 3.0: Apply mobile device security strategies including remote wipe, biometrics, and device access controls.

==========

QUESTION 205

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned

A. An on-premises solution as a backup

B. A load balancer with a round-robin configuration

C. A multicloud provider solution

Answer: D. An active-active solution within the same tenant C

Multicloud provider solutionsinvolve using services from more than one cloud provider to ensure resiliency and redundancy. In the event of a failure or SLA breach by one CSP, another provider can maintain service continuity. An on-premises backup could help, but does not address CSP-specific SLA concerns directly. Round-robin load balancing and active-active within the same tenant still depend on a single provider, thus posing risks if the CSP fails.

Reference:CompTIA SecurityX CAS-005, Domain 4.0: Implement redundancy and fault-tolerant strategies, including multicloud deployment for service resiliency.

QUESTION 206

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

Answer: F. Geotagging A,D

Geofencingallows the device to be restricted based on its physical location ” disabling or locking devices when they move outside of trusted zones.Full disk encryptionensures 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.

==========

QUESTION 207

Which of the following security risks should be considered as an organization reduces cost and increases availability of services by adopting serverless computing?

A. Level of control and influence governments have over cloud service providers

B. Type of virtualization or emulation technology used in the provisioning of services

C. Vertical scalability of the infrastructure underpinning the serverless offerings

Answer: D. Use of third-party monitoring of service provisioning and configurations A

In serverless computing, organizations rely heavily on CSPs to manage the infrastructure, runtime, and scaling. A key risk is thelevel of control and influence governments have over CSPs, potentially affecting availability, access, or confidentiality of hosted services due to legal orders or government actions. Concerns about virtualization technologies, scalability, or third-party monitoring are valid but less critical compared to the overarching legal and control risks tied to CSP reliance.

Reference:CompTIA SecurityX CAS-005, Domain 4.0: Understand the legal and regulatory impacts and risks of adopting third-party serverless solutions.

QUESTION 208

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

Answer: D. Supply chain attack D

This scenario clearly describes asupply 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.

==========

QUESTION 209

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

Answer: D. Utilize HMAC for the keys D

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:CompTIA SecurityX CAS-005, Domain 3.0: Implement secure API practices including the use of HMAC for key protection.

==========

QUESTION 210

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. Local drive encryption

B. Secure boot

C. Address space layout randomization

D. Unneeded services disabled

E. Patching

F. Logging

G. Removal of unused accounts

Answer: H. Enabling BIOS password D,E,G

Disabling unneeded servicesreduces the attack surface by closing open ports.Patchingensures that endpoint protection software and operating systems are up-to-date, reducing vulnerability exposure.Removing unused accountseliminates access paths for malicious users exploiting dormant accounts. Secure boot, BIOS passwords, and drive encryption are important, but they address different layers of security than the vulnerabilities listed.

Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply system hardening techniques to endpoint security issues.

==========

QUESTION 211

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. CVE

B. CVSS

C. CCE

D. CPE

Answer: A

CVE (Common Vulnerabilities and Exposures)provides unique identifiers for publicly known cybersecurity vulnerabilities and exposures. Each CVE entry includes a description and, often, remediation information. CVSS refers to scoring severity, CCE focuses on configuration issues, and CPE deals with naming standardized platforms and systems.

Reference:CompTIA SecurityX CAS-005, Domain 2.0: Utilize publicly available vulnerability sources like CVE for risk mitigation.

==========

QUESTION 212

A security analyst notices a number of SIEM events that show the following activity: 100 - 8:01 UTC - 192.168.1.1 - sc stop HinDctend

100 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptidcasp.exe 100 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell 100 - 8:07 UTC - 192.168.1.1 - powershell ”> 40.90.23.154:443

Which of the following response actions should the analyst take first?

B. Restart Microsoft Windows Defender

C. Configure the forward proxy to block 40.90.23.154

Answer: D. Disable local administrator privileges on the endpoints C

The first immediate action in an active incident iscontainment.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.

Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply incident response techniques focusing on immediate containment actions.

QUESTION 213

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

Answer: D. Camellia-CBC C

ChaCha20-Poly1305is 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

==========

QUESTION 214

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

Answer: E. Incinerating E

For SSDs,incinerationis 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:CompTIA SecurityX CAS-005, Domain 2.0: Apply secure media sanitization methods appropriate for device types such as SSDs.

==========

QUESTION 215

A healthcare system recently suffered from a ransomware incident. As a result, the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits, and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would best solve these challenges? (Select three).

A. SD-WAN

B. PAM

C. Remote access VPN

D. MFA

E. Network segmentation

F. BGP

G. NAC

Answer: B,D,E

Privileged Access Management (PAM)restricts elevated permissions, reducing the risk of widespread ransomware attacks.Multi-Factor Authentication (MFA)protects against credential theft and ensures that even if passwords are compromised, accounts are not easily accessible.Network

segmentationbreaks the flat network into secure zones, limiting lateral movement by attackers. SDWAN and BGP relate to network routing and efficiency, not security architecture specifically. Remote

access VPN secures external access but does not solve internal flat network issues. Network Access Control (NAC) is helpful but secondary compared to PAM, MFA, and segmentation in this context. Reference:CompTIA SecurityX CAS-005, Domain 2.0: Implement identity and access controls, network segmentation, and authentication hardening to mitigate internal threats.

QUESTION 216

An organization recently implemented a policy that requires all passwords to be rotated every 90 days. An administrator observes a large volume of failed sign-on logs from multiple servers that are often accessed by users. The administrator determines users are disconnecting from the RDP session but not logging off. Which of the following should the administrator do to prevent account lockouts?

A. Increase the account lockout threshold.

B. Enforce password complexity.

C. Automate logout of inactive sessions.

D. Extend the allowed session length.

Answer: C

When users disconnect from Remote Desktop Protocol (RDP) sessions without properly logging off, their sessions remain active on the server. If their passwords are changed due to the 90-day rotation policy, these lingering sessions may attempt to reauthenticate using outdated credentials, leading to multiple failed login attempts and potential account lockouts.

Automating the logout of inactive sessions ensures that disconnected or idle sessions are terminated after a specified period, preventing stale sessions from causing authentication issues. This approach aligns with best practices for session management and helps maintain security compliance.

Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: "Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment."

QUESTION 217

A security engineer wants to improve the security of an application as part of the development pipeline. The engineer reviews the following component of an internally developed web application that allows employees to manipulate documents from a number of internal servers:

response = requests.get(url)

A. Indexing

B. Output encoding

C. Code scanner

D. Penetration testing

Answer: C

The application allows users to input URLs, which the application then fetches using requests.get(url). This functionality can be exploited if not properly validated, leading to potential security vulnerabilities such as Server-Side Request Forgery (SSRF).

Implementing a code scanner as part of the development pipeline can help identify insecure coding practices, such as unsanitized user inputs and improper handling of external requests. Code scanners analyze the source code for known vulnerabilities and coding errors, enabling developers to remediate issues before deployment.

Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 2.2: "Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages."

QUESTION 218

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.

Answer: C,D

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."

QUESTION 219

Which of the following tests explains why AI output could be inaccurate?

A. Model poisoning

B. Social engineering

C. Output handling

Answer: D. Prompt injections A

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 doesnt 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.

A software vendor provides routine functionality and security updates to its global customer base. The vendor would like to ensure distributed updates are authorized, originate from only the company, and have not been modified by others. Which of the following solutions best supports these objectives?

A. Envelope encryption

B. File integrity monitoring

C. Application control

Answer: D. Code signing D

Code signing uses cryptographic digital signatures to prove that software or updates come from a trusted source and have not been altered. In the SecurityX CAS-005 objectives, this is covered under security engineering and cryptographic assurance mechanisms.

Envelope encryption protects confidentiality but does not authenticate the source.

File integrity monitoring detects file changes but does not confirm the origin of the update. Application control manages which software can run but does not ensure authenticity of distributed files.Only code signing meets all three objectives: verifying the source, ensuring authorization, and proving integrity.

QUESTION 221

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

Answer: D. Using a software dependency management solution D

SecurityX CAS-005 exam content emphasizes integrating security into the SDLC and using automated tools to identify vulnerabilities early.

Software dependency management solutions track and analyze libraries and components for known vulnerabilities before deployment, using vulnerability databases such as NVD or OSS Index.

IAST scanning still requires the application to be running and may detect issues later.

SIEM monitoring is reactive and identifies issues after they occur.By detecting vulnerable dependencies early, software dependency management solutions prevent late-stage deployment delays and reduce security risk.

QUESTION 222

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

Answer: D. Scanning the application with SAST B

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.

QUESTION 223

A global organization is reviewing potential vendors to outsource a critical payroll function. Each vendor's plan includes using local resources in multiple regions to ensure compliance with all regulations. The organization's Chief Information Security Officer is conducting a risk assessment on the potential outsourcing vendors' subprocessors. Which of the following best explains the need for

A. Risk mitigations must be more comprehensive than the existing payroll provider.

B. Due care must be exercised during all procurement activities.

C. The responsibility of protecting PII remains with the organization.

D. Specific regulatory requirements must be met in each jurisdiction.

Answer: C

Per SecurityX CAS-005 GRC principles, outsourcing a function does not transfer accountability for protecting personally identifiable information (PII). While subprocessors handle data, the originating organization remains responsible under most data protection laws and frameworks (e.g., GDPR, CCPA).

Due care in procurement (option B) is important, but it is a supporting concept, not the primary driver in this context.

Jurisdictional compliance (option D) is a requirement, but the underlying reason for risk assessment is that accountability for PII protection remains with the organization.

QUESTION 224

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

Answer: D. Deploying a honeypot D

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.

A network security architect for an organization with a highly remote workforce implements an always-on VPN to meet business requirements. Which of the following best explains why the architect is using this approach?

A. To facilitate device authentication using on-premises directory services

B. To allow access to directly connected print and scan resources

C. To enable usability of locally attached removable storage

Answer: D. To authorize updates to change the PIN on a smart card A

Always-on VPN ensures that devices connect automatically to the corporate network whenever they

are online, allowing seamless access to internal resources and enabling authentication against onpremises directory services (such as Active Directory). This supports centralized identity

management, GPO enforcement, and compliance requirements.

Options B, C, and D involve local or peripheral resources, which are unaffected by VPN state.

QUESTION 226

A user tried to access a web page at http:/.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. Implementing 802.1x EAP-TTLS on access points to reduce the risk of evil twins

B. Transitioning internal services to use DNS security

C. Modifying web server configuration and utilizing X509 certificates for authentication

Answer: D. Installing new rules for the IDS to detect impersonation attacks C

Using X.509 certificates for authentication with HTTPS encrypts credentials in transit and provides server identity verification. In SecurityX CAS-005 objectives, securing internal web services with TLS and mutual authentication is a primary method to reduce credential interception or reuse.

802.1X EAP-TTLS is for network access control, not web authentication. DNS security (DNSSEC) ensures DNS integrity, not web session encryption. IDS rules help detect, but not prevent, credential exposure.

QUESTION 227

A large organization deployed a generative AI platform for its global user population to use. Based on feedback received during beta testing, engineers have identified issues with user interface latency

A. Configuring the application to use a CDN

B. Implementing RASP to enable large language models queuing

C. Remote journaling within a third data center

Answer: D. Traffic shaping through the use of a SASE A

A Content Delivery Network (CDN) caches and distributes static and dynamic web content across multiple geographically distributed edge servers, reducing latency for global users. This directly addresses page-loading delays caused by distance from the primary data centers.

RASP is for runtime application security, not latency.

Remote journaling is for data replication, not performance optimization.

SASE can improve security and WAN routing, but a CDN is purpose-built for content delivery performance.

QUESTION 228

A systems administrator is working with clients to verify email-based services are performing properly. The administrator wants to have the email server digitally sign outbound emails using the organization's private key. Which of the following should the systems administrator configure?

A. SPF

B. DKIM

C. DMARC

D. TLS

Answer: B

DomainKeys Identified Mail (DKIM) digitally signs outbound messages with the organizations private key, enabling recipients to verify integrity and authenticity using the corresponding public key in DNS.

SPF validates sending server IPs, not message integrity.

DMARC builds policy enforcement on top of SPF and DKIM results. TLS secures the transport channel, not the message content itself.

QUESTION 229

An administrator brings the company's fleet of mobile devices into its PKI in order to align device

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

Answer: F. Submitting a CSR to the CA to obtain a single certificate that can be used across all devices A,E

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.

QUESTION 230

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

SecurityX CAS-005 emphasizes automation with validation in security operations. Security Orchestration, Automation, and Response (SOAR) platforms can integrate with Threat Intelligence

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.

QUESTION 231

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

Answer: D. Internal reconnaissance A

Adversary emulation simulates specific advanced persistent threat (APT) behaviors and techniques to

test an organizations security posture. In SecurityX CAS-005, this is part of red-teaming and purpleteaming 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.

QUESTION 232

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

Answer: D. Deploying microsegmentation with a firewall acting as the core router A

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.

QUESTION 233

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. The analyst has previous work experience in application development.

B. Sufficient metrics are not available to conduct other risk assessment types.

C. An organizational risk register tracks all risks and mitigations across business units.

D. The organization wants to find the monetary value of any outages.

Answer: B

Qualitative risk assessment is used when quantitative data (monetary loss, exact downtime cost, RTO) is unavailable or unreliable. The SecurityX CAS-005 GRC objectives note that qualitative methods rely on expert judgment, likelihood scales, and impact ratings rather than financial calculations. In this case, insufficient metrics rule out quantitative analysis.

Option A (work experience) is irrelevant to the choice of assessment type. Option C (risk register) supports tracking, not selecting the assessment method.

Option D describes a quantitative goal, which is not possible with the given lack of metrics.

QUESTION 234

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.

C. Implement a load balancer for computing and storage resources.

D. Plan for a horizontally scaling computing and storage infrastructure.

Answer: D

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.

QUESTION 235

A subcontractor develops safety critical avionics software for a major aircraft manufacturer. After an incident, a third-party investigator recommends the company begin to employ formal methods in the development life cycle. Which of the following findings from the investigation most directly supports the investigator's recommendation?

A. The system's bill of materials failed to include commercial and open-source libraries.

B. The company lacks dynamic and Interactive application security testing standards.

C. The codebase lacks traceability to functional and non-functional requirements.

D. The implemented software inefficiently manages compute and memory resources.

Answer: C

Formal methods in software engineering use mathematically based specifications to ensure system correctness, safety, and compliance with requirements. SecurityX CAS-005 stresses the importance of traceability between code and both functional and non-functional requirements for high-assurance systems like avionics. A lack of traceability means it is impossible to verify that the implementation meets all required safety and performance standards”exactly what formal methods address.

QUESTION 236

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

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: C

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.

Option D is reactive and does not prevent insecure deployments.

QUESTION 237

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

Answer: D. Deploying fake ransomware C

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.

QUESTION 238

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?

B. Implementing the NIDS and the NIPS together with the main firewall

C. Implementing a NIDS without a NIPS to increase the detection capability

Answer: D. Implementing the NIDS in the bastion host and the NIPS in the branch network router A

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.

QUESTION 239

An organization recently migrated data to a new file management system. The architect decides to use a discretionary authorization model on the new system. Which of the following best explains the architect's choice?

A. The responsibility of migrating data to the new file management system was outsourced to the vendor providing the platform.

B. The permissions were not able to be migrated to the new system, and several stakeholders were made responsible for granting appropriate access.

C. The legacy file management system did not support modern authentication techniques despite the business requirements.

D. The data custodians were selected by business stakeholders to ensure backups of the file management system are maintained off site.

Answer: B

In a Discretionary Access Control (DAC) model, the data owner or an assigned stakeholder has the authority to determine who can access resources. SecurityX CAS-005 IAM objectives describe DAC as user- or owner-controlled, where permissions can be granted or revoked at the owners discretion.

In this scenario, because permissions from the legacy system could not be migrated, multiple stakeholders were made responsible for assigning and managing access”matching the DAC models characteristics.

Option A relates to outsourcing, which does not define an access control model. Option C is about authentication limitations, unrelated to the choice of DAC.

Option D describes backup responsibilities, which are operational tasks, not access control.

During a recent audit, a company's systems were assessed- Given the following information:

Department	System	Status	Notes
Accounting	TaxReporting	OK	
Human resources	HRIS	OK	
Manufacturing	ProductionControl	WARNING	EOL software detected
Support	ServiceDesk	WARNING	Patches available

Which of the following is the best way to reduce the attack surface?

A. Deploying an EDR solution to all impacted machines in manufacturing

B. Segmenting the manufacturing network with a firewall and placing the rules in monitor mode

C. Setting up an IDS inline to monitor and detect any threats to the software

Answer: D. Implementing an application-aware firewall and writing strict rules for the application access D

SecurityX CAS-005 network architecture objectives emphasize limiting exposure of vulnerable systems by using application-aware firewalls with strict rule sets.

This approach directly reduces the attack surface by allowing only approved application traffic to and from the vulnerable systems, mitigating risk until systems are patched or replaced.

EDR (A) enhances detection but doesnt inherently reduce the exposed services. Network segmentation in monitor mode (B) doesnt block threats.

IDS (C) detects activity but does not block it.

QUESTION 241

A building camera is remotely accessed and disabled from the remote console application during offhours. 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

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

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.

QUESTION 242

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

Answer: D. Crisis management plan D

A crisis management plan defines coordinated communication and response strategies for highprofile incidents that may harm an organizations public reputation and shareholder confidence. CAS-

A Data Subject Access Request (A) addresses individual data rights, not overall crisis handling. Business Impact Analysis (B) helps assess potential operational and financial impacts but does not manage public perception during an incident.

Supply chain management (C) is preventative for vendor risks, not responsive to current crises.

QUESTION 243

A web application server that provides services to hybrid modern and legacy financial applications recently underwent a scheduled upgrade to update common libraries, including OpenSSL. Multiple users are now reporting failed connection attempts to the server. The technician performing initial triage identified the following:

Client applications more than five years old appear to be the most affected. Web server logs show initial connection attempts by affected hosts.

For the failed connections, logs indicate "cipher unavailable."

Which of the following is most likely to safely remediate this situation?

A. The server needs to be configured for backward compatibility to SSL 3.0 applications.

B. The client applications need to be modified to support AES in Galois/Counter Mode or equivalent.

C. The client TLS configuration must be set to enforce electronic codebook modes of operation.

D. The server-side digital signature algorithm needs to be modified to support elliptic curve cryptography.

Answer: B

The œcipher unavailable message indicates that the client and server could not agree on a common cipher suite. After the OpenSSL update, the server likely dropped support for older, insecure ciphers (such as RC4 or 3DES) that legacy clients still use. The safest remediation is to update or configure the client applications to support modern, secure ciphers such as AES in Galois/Counter Mode (AESGCM) or an equivalent strong cipher suite that is supported by the updated OpenSSL server.

Option A (SSL 3.0) is unsafe because SSL 3.0 is deprecated and vulnerable to multiple attacks (e.g., POODLE).

Option C (ECB mode) is insecure due to pattern leakage and should never be enforced.

Option D (ECC signatures) relates to key exchange and signatures, not to the œcipher unavailable issue directly.

This approach aligns with SecurityX CAS-005 cryptographic interoperability guidance”modernize clients rather than reintroduce insecure protocols.

QUESTION 244

A security analyst is reviewing a SIEM and generates the following report:

Log source	Destination IP	Source IP	Hostname	Event ID	Action	Time
DEV001	192.168.1.2	192.168.2.2	VM001	9928	Deny connection	4:55:28
DEV001	192.168.3.2	192.168.2.2	VM001	1912	IPS Alert	7:21:41
DEV001	10.1.1.1,192.168.2.2,VM001,1822 Malware detection,8:11:12					
DEV001	10.1.1.1	192.168.2.2	VM001	9927	Allow connection	8:15:32

Later, the incident response team notices an attack was executed on the VM001 host. Which of the following should the security analyst do to enhance the alerting process on the SIEM platform?

A. Include the EDR solution on the SIEM as a new log source.

B. Perform a log correlation on the SIEM solution.

C. Improve parsing of data on the SIEM.

D. Create a new rule set to detect malware.

Answer: B

The SIEM already contains multiple events that, if correlated, would have indicated an active attack sequence on VM001”such as denied connections, IPS alerts, malware detection, and then an allowed connection. CAS-005 Security Operations objectives emphasize log correlation as a way to enhance detection by linking related events across different time stamps and data sources into a single, higher-confidence alert.

Option A (adding EDR logs) could add visibility but does not address the need to connect existing events for earlier detection.

Option C (improving parsing) ensures readability but does not create actionable alerts.

Option D (creating a new malware detection rule) is redundant since malware detection already appeared in logs; the issue was the lack of correlation to act on it in time.

By correlating IDS, IPS, firewall, and malware detection logs, the SIEM can raise a higher-priority alert before the attack is completed.

QUESTION 245

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

Answer: D. Certificate extension A

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. œCertificate extension (D) is a generic term; SAN is the specific required extension.

QUESTION 246

An organization purchased a new manufacturing facility and the security administrator needs to: Implement security monitoring.

Protect any non-traditional device(s)/network(s). Ensure no downtime for critical systems.

Which of the following strategies best meets these requirements?

A. Configuring honeypots in the internal network to capture malicious activity

B. Analyzing system behavior and responding to any increase in activity

C. Applying updates and patches soon after they have been released

D. Observing the environment and proactively addressing any malicious activity

Answer: D

For operational technology (OT) and non-traditional devices, downtime must be avoided. CAS-005 recommends passive monitoring and proactive response for environments where active scanning or changes could disrupt operations. Observing the environment continuously and acting on malicious indicators allows security without interrupting critical manufacturing processes.

Honeypots (A) are good for research but dont provide full facility monitoring. Behavioral analysis (B) is reactive without proactive measures.

Patching (C) is important but could cause downtime and may be limited in OT environments.

QUESTION 247

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

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

Answer: D. Resyncing single sign-on application with connected security appliances B

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.

QUESTION 248

After a cybersecurity incident, a security analyst was able to collect a binary that the attacker used on the compromised server. Then the analyst ran the following command:

Which of the following options describes what the analyst is trying to do?

A. To reconstruct the timeline of commands executed by the binary

B. To extract IoCs from the binary used on the attack

Answer: C. To replicate the attack in a secure environment B

The strings utility extracts human-readable text from binary files. Security analysts use it to identify Indicators of Compromise (IoCs) such as URLs, IP addresses, filenames, and commands embedded in the malware.

Option A (reconstructing timeline) would require event logs or forensic timeline tools. Option C (replicating the attack) involves execution in a sandbox, not static string extraction.

QUESTION 249

A company needs to quickly assess whether software deployed across the company's global corporate network contains specific software libraries. Which of the following best enables the company's SOC to respond quickly when such an assessment is required?

A. Maintaining SAST/DAST reports on a server with access restricted to SOC staff

B. Contractually requiring all software vendors to attest to third-party risk mitigations

Answer: D. Implementing a GRC tool to maintain a list of all software vendors and internal developers C

The best way for a SOC to rapidly identify whether deployed applications contain specific libraries is through the use of a Software Bill of Materials (SBOM). An SBOM is a formal, machine-readable inventory of all components, including third-party and open-source libraries, used in a software product. When a new vulnerability is disclosed (such as Log4Shell in Log4j), organizations with a comprehensive SBOM can immediately search across their application landscape to determine which systems are impacted.

Other options are less effective. Maintaining SAST/DAST reports (A) only provides snapshots of vulnerabilities at the time of scanning, but does not dynamically track components across all software in production. Vendor attestations (B) improve supply chain governance but do not provide

immediate visibility into internal or custom software. A GRC tool (D) helps track vendors and policies but does not show technical dependencies inside applications.

Requiring suppliers and internal developers to provide and maintain SBOMs ensures continuous visibility into dependencies. This allows the SOC to quickly query and respond to emerging vulnerabilities, reducing risk exposure and accelerating remediation timelines.

QUESTION 250

Engineers are unable to control pumps at Site A from Site B when the SCADA controller at Site A experiences an outage. A security analyst must provide a secure solution that ensures Site A pumps can be controlled by a SCADA controller at Site B if a similar outage occurs again. Which of the following represents the most cost-effective solution?

A. Procure direct fiber connectivity between Site A and Site B and limit its use to the critical SCADA controller traffic only

B. Install backup SCADA controllers at each site, isolate them from the OT network, and assign these backup controllers as high-availability pairs.

C. Isolate the OT environment by providing an air-gapped network segment. Place the SCADA controller for each site in this network segment to minimize outages.

D. Configure VPN concentrators inside the OT network segments at Site A and Site B and allow the controllers to act as secondary devices for the other site's pumps across this encrypted tunnel.

Answer: D

The most cost-effective and secure solution is to configure VPN concentrators inside the OT networks at both sites (Option D). This setup allows encrypted communications between Site A and Site B, enabling controllers at either site to serve as secondary or failover devices for the other. By

Option A, direct fiber connectivity, provides high performance but is extremely costly and less flexible than VPN solutions. Option B, deploying redundant SCADA controllers at each site, increases hardware, licensing, and management costs while still requiring interconnectivity. Option C, airgapping the OT network, may improve isolation but would prevent remote failover capabilities,

contradicting the requirement for cross-site control.

By implementing VPN concentrators, the organization achieves secure cross-site redundancy, supports operational continuity in case of controller outages, and does so in a cost-effective manner aligned with common OT security practices.

QUESTION 251

During a recent security event, access from the non-production environment to the production environment enabled unauthorized users to install unapproved software and make unplanned configuration changes. During an investigation, the following findings are identified:

Several new users were added in bulk by the IAM team.

Additional firewalls and routers were recently added to the network.

Vulnerability assessments have been disabled for all devices for more than 30 days. The application allow list has not been modified in more than two weeks.

Logs were unavailable for various types of traffic. Endpoints have not been patched in more than ten days.

Which of the following actions would most likely need to be taken to ensure proper monitoring is in place within the organization? (Select two)

A. Disable bulk user creations by the IAM team.

B. Extend log retention for all security and network devices for 180 days for all traffic.

C. Review the application allow list on a daily basis to make sure it is properly configured.

D. Routinely update all endpoints and network devices as soon as new patches/hot fixes are available.

E. Ensure all network and security devices are sending relevant data to the SIEM.

F. Configure rules on all firewalls to only allow traffic from the production environment to the nonproduction environment.

Answer: B,E

The incident highlights gaps in visibility, monitoring, and log management that allowed unauthorized access to persist undetected. The most critical corrective actions are to extend log retention for all devices (B) and to ensure all devices are

forwarding relevant logs to the SIEM (E). Together, these steps strengthen monitoring and incident detection capabilities by ensuring that sufficient telemetry is collected, stored, and available for correlation and investigation.

By prioritizing comprehensive log collection and ensuring adequate retention, the SOC can correlate anomalies across systems, detect malicious behavior earlier, and conduct forensic investigations effectively. This aligns with CAS-005 best practices for security operations and continuous monitoring in hybrid environments.

QUESTION 252

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 â† 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

The routing entry 0.0.0.0/0 forces all traffic from remote clients"including traffic destined for the public internet"through the VPN tunnel. This is called full-tunnel VPN routing. While it ensures strong security by forcing all traffic to pass through corporate controls, it can also overload VPN gateways and cause slow access to both internal and external applications, as seen in this scenario. The correct fix is to enable split tunneling (B). Split tunneling allows only corporate traffic (e.g., private IP ranges or internal applications) to flow through the VPN, while internet-bound traffic routes directly to the internet. This reduces congestion on VPN concentrators, improves performance for remote users, and ensures efficient use of bandwidth.

Moving servers to a screened subnet (A) relates to internal segmentation but does not fix the VPN bottleneck. NAC (C) enforces device compliance but does not address routing inefficiencies. DNS over HTTPS (D) secures name resolution but is unrelated to network congestion.

Thus, enabling split tunneling balances security and performance for remote workers.

QUESTION 253

A security architect is performing threat-modeling activities related to an acquired overseas software company that will be integrated with existing products and systems Once its software is integrated, the software company will process customer data for the acqumng company Given the following:

ID	Threat	STRIDE	Criticality
01	Attacker performs denial of service against public-facing endpoints	Denial of service	High
02	Malicious insider puts a backdoor into source code	Tampering	Critical
03	Attacker injects malicious code into third-party library	Tampering	Critical
04	Attacker escalates privilege to administrator in web system	Elevation of privilege	High
05	Attacker performs successful password spraying	Spoofing	High

Which of the following mitigations would reduce the risk of the most significant threats?

A. Privileged access management system with conditional access capabilities to prevent unauthorized access

B. Rate-limiting capabilities on all authentication systems and leveraging single sign-on through federation

C. Secure development process with gate checks and appropriate code scanning

D. Zero Trust architecture for all assets from the acquired company using microsegmentation against sensitive applications

Answer: C

The table highlights that tampering threats (IDs 02 and 03) are rated Critical, making them the most

significant risks. These threats involve malicious insiders inserting backdoors or attackers injecting malicious code into third-party libraries. To mitigate such risks, organizations must implement a secure software development lifecycle (SDLC) with formalized code scanning, gate checks, and supply chain validation.

Option C directly addresses these issues. Secure development practices include static/dynamic code analysis, dependency checks, peer reviews, and mandatory approvals before code promotion. This approach detects backdoors, prevents unauthorized modifications, and reduces the likelihood of compromised libraries being integrated.

Option A (PAM with conditional access) mitigates privilege escalation but does not address software tampering. Option B (rate limiting and federation) reduces brute-force authentication risks (ID 05) but not critical tampering. Option D (Zero Trust with microsegmentation) strengthens network defense but does not secure the integrity of source code or libraries.

Therefore, a secure SDLC with gate checks and code scanning is the best mitigation for the most critical threats identified.

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: B

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.

QUESTION 255

A company SIEM collects information about the log sources. Given the following report information:

Which of the following actions should a security engineer take to enhance the security monitoring posture?

A. Calibrate the timing on the log sources to enhance event correlation.

B. Implement a centralized use case library to get alerts based on the type of log sources.

C. Perform a non-reporting device assessment to collect missing log sources.

D. Create a resiliency plan to prevent losing event logs from log sources.

Answer: C

The SIEM report shows that some devices, such as VM003 (Critical server) and NET003 (IPS), are DOWN and therefore not reporting logs. In security monitoring, the absence of log data from critical systems creates dangerous blind spots. If logs are missing, attacks can proceed undetected, or investigations may lack the data needed for incident response.

The most effective action is to perform a non-reporting device assessment (C). This means identifying and correcting issues where devices fail to send logs, whether due to outages, misconfigurations, or integration gaps. Ensuring all critical devices, especially servers and intrusion prevention systems, consistently send logs to the SIEM strengthens overall visibility and monitoring posture.

Option A (time calibration) is important for correlation accuracy but does not address missing log feeds. Option B (centralized use case library) enhances detection but only works if the SIEM is receiving complete data. Option D (resiliency plan) helps protect log retention but is irrelevant if logs are never received in the first place.

Therefore, fixing non-reporting log sources is the highest priority to improve monitoring effectiveness.

QUESTION 256

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.

C. Enforce daily posture compliance checks against the endpoint security controls.

D. Deploy context-aware reauthentication with UBA baseline deviations.

Answer: D

Zero Trust security is based on the principle of œnever 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, riskbased 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.

By starting with context-aware reauthentication, the organization ensures its Zero Trust strategy adapts dynamically to user behavior, providing both stronger security and a smoother experience for a global, remote workforce.

QUESTION 257

A company has the following requirements for a cloud-based web application: Must authenticate customers

Must prevent data exposure

Must allow customer access to data throughout the cloud environment Must restrict access by specific regions

Which of the following solutions best addresses these security requirements?

A. Applying role-based access controls and configuring geolocation policies

B. Replicating the data in each customer environment

C. Hosting the data regionally and providing each customer with a unique link

Answer: D. Moving to a cloud provider that operates only in one specific region A

The best way to address these requirements is to apply Role-Based Access Controls (RBAC) combined with geolocation policies. RBAC ensures that customers are authenticated and authorized to access only the data they are entitled to, thereby minimizing data exposure risks. At the same time, geolocation policies enforce restrictions on which regions customers can access data from, helping

Option B (replicating data in each customer environment) is inefficient, expensive, and introduces additional risks related to data sprawl. Option C (regional hosting with unique links) complicates access management and does not inherently prevent exposure or enforce strong authentication.

Option D (restricting to a single region provider) removes flexibility and may conflict with customer needs for global access.

Therefore, implementing RBAC along with geolocation controls provides fine-grained access management, ensures compliance, prevents unnecessary data exposure, and is scalable for a global cloud environment.

QUESTION 258

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 DSS self-assessment questionnaire.

Answer: C

The most likely driver for approving additional network security budget is that the audit revealed that the existing architecture contained security controls that could be easily bypassed. This indicates fundamental weaknesses in defense-in-depth and suggests that attackers could gain access to sensitive systems or data despite the presence of controls.

Option A (unused budgets) is not a strategic reason for approving security investment. Option B (compliance reports requested by customers) may influence investment in compliance initiatives, but it does not explain the need for an in-depth defense architecture. Option D (PCI DSS low score) is a compliance-specific issue but would not, on its own, drive a broad architectural budget approval unless PCI was the only focus.

Security audits often uncover systemic flaws”such as flat networks, insufficient segmentation, or single points of failure”that create the conditions for bypassing controls. Addressing these issues requires rearchitecting the environment, introducing layered defenses, and strengthening monitoring capabilities, all of which demand significant budget. Thus, option C aligns with the decision to invest in robust defense-in-depth strategies.

QUESTION 259

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

A. Mitigation

B. Impact

C. Likelihood

D. Appetite

Answer: D

The CIO needs to clarify the organizations risk appetite, which defines the level of residual risk the business is willing to accept after all mitigation measures are applied. Risk appetite reflects the balance between operational requirements, security controls, and cost constraints. In business continuity planning, risk appetite helps decision-makers determine which risks must be reduced through additional investments (e.g., redundant systems, faster recovery strategies) and which risks are tolerable based on business priorities.

Mitigation (A) refers to the strategies used to reduce risk but not the threshold of acceptable residual risk. Impact (B) and Likelihood (C) are components of risk assessment”measuring severity and probability”but they do not define acceptance criteria. Risk appetite is the guiding principle that aligns technical controls with executive tolerance for disruption or loss.

By clarifying appetite, the CIO provides the compliance team and IT leadership with a framework for designing remediation activities that ensure continuity of critical internal processes while aligning with the organizations strategic objectives and regulatory requirements.

QUESTION 260

Which of the following includes best practices for validating perimeter firewall configurations?

A. CIS controls

B. MITRE ATT&CK

C. NIST CSF

D. ISO 27001

Answer: A

The Center for Internet Security (CIS) Controls provide prescriptive best practices for validating and securing perimeter firewalls. These controls are specifically designed to offer detailed, actionable steps that organizations can follow to ensure

firewall rules are configured properly, access is restricted to least privilege, and unnecessary services are disabled. CIS benchmarks also provide specific configuration guidance for different vendors, making them highly practical for real-world implementation and validation.

Therefore, the CIS Controls and Benchmarks represent the most direct and practical resource for validating firewall configurations in line with recognized industry best practices.

QUESTION 261

A malicious actor exploited firmware vulnerabilities and used rootkits in an attack on an organization. After the organization recovered from the incident, an engineer needs to recommend a solution that reduces the likelihood of the same type of attack in the future. Which of the following is the most relevant solution?

A. Enabling software integrity checks

B. Installing self-encrypting drives

C. Implementing measured boot

Answer: D. Configuring host-based encryption C

The best solution to reduce the likelihood of firmware-level attacks and rootkits is to implement measured boot. Measured boot is a hardware-assisted security mechanism that leverages Trusted Platform Module (TPM) and Secure Boot processes. It records cryptographic measurements of each stage of the boot process”from firmware to operating system loaders”and stores them in the TPM. Security software, such as attestation services, can then verify that the system booted into a known, trusted state. If firmware or boot-level code has been tampered with, the measurements will not match expected values, alerting administrators to compromise.

Option A (software integrity checks) validates application-level integrity but does not address firmware rootkits that load before the operating system. Option B (self-encrypting drives) protects data at rest but does not prevent rootkits. Option D (host-based encryption) ensures confidentiality but does not detect or mitigate firmware-level persistence.

Measured boot specifically targets low-level tampering, making it the most relevant control to defend against rootkits and firmware exploits.

QUESTION 262

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

C. Terraform

D. Ansible

Answer: C

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.

QUESTION 263

A company detects suspicious activity associated with inbound 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: A

The best solution is to implement an interactive honeypot (A). Honeypots are decoy systems designed to attract and observe adversary behavior in real time. When security tools cannot categorize suspicious inbound traffic, a honeypot provides an isolated environment where the

suspicious activity can be redirected and monitored without risking production systems. By deploying an interactive honeypot, analysts can study attacker tactics, techniques, and procedures (TTPs), extract Indicators of Compromise (IoCs), and improve defensive controls.

Option B (mapping to known IoCs) fails because the activity cannot be categorized, implying it is

Option D (UEBA) focuses on analyzing user and entity behaviors but is less effective for categorizing inbound external traffic.

By using honeypots, organizations gain visibility into new, unknown, or advanced attack techniques, which helps improve detection capabilities, enrich threat intelligence, and strengthen incident response.

QUESTION 264

Based on the results of a SAST report on a legacy application, a security engineer is reviewing the following snippet of code flagged as vulnerable:

```
[01] #include <stdio.h>
[02] #include <string.h>
[03] ...
[04]  char input[256] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
[05]  ...
[06]  char transmit[20] = "0000";
[07]  char *ret_xmit;
[08]  printf("To be submitted: \"%s\"\n", input);
[09]  result in ret_xmit
[10]  ret_xmit = strcpy(transmit, input);
[12]  return 0;
[13] }
```

Which of the following is the vulnerable line of code that must be changed?

A. Line (02]

B. Line [04]

C. Line [07]

D. Line 108]

Answer: E. Line [10] E

The vulnerability lies in line [10], where the function strcpy(transmit, input) is used. The strcpy function does not perform boundary checking when copying strings. Since input is defined with a size of 256 characters and transmit only has 20 characters allocated, the strcpy operation will cause a buffer overflow when the contents of input exceed the allocated size of transmit. This creates a significant security vulnerability, as attackers can overwrite adjacent memory, potentially injecting malicious code or altering program execution.

Lines [02], [04], [07], and [08] are not inherently vulnerable by themselves. Line [04] defines the oversized input, but the vulnerability only materializes when combined with the unsafe copy in line

Thus, the vulnerable line that must be changed is line [10], where strcpy is used.

QUESTION 265

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

Answer: F. Security runbook B,D

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 dont 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.

QUESTION 266

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?

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

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.

By automating golden image creation through Terraform, the company gains efficiency, repeatability, and security assurance, aligning with DevSecOps principles and CAS-005 cloud-native best practices.

QUESTION 267

A threat intelligence company's business objective is to allow customers to integrate data directly to different TIPs through an API. The company would like to address as many of the following objectives as possible:

Reduce compute spend as much as possible. Ensure availability for all users.

Reduce the potential attack surface. Ensure the integrity of the data provided.

Which of the following should the company consider to best meet the objectives?

A. Configuring a unique API secret key for accounts

B. Publishing a list of IoCs on a public directory

C. Implementing rate limiting for each registered user

Answer: D. Providing a hash of all data that is made available D

The best solution is to provide a hash of all data made available (D). Hashing ensures the integrity of the threat intelligence data provided to customers. Clients can verify that the data received via API

Option A (API secret keys) improves authentication and reduces attack surface but does not address integrity or compute efficiency. Option B (publishing IoCs publicly) increases attack surface and reduces control over distribution, which conflicts with security objectives. Option C (rate limiting) helps availability and cost control but does not guarantee data integrity.

By providing hashes, the company ensures customers can validate authenticity regardless of delivery method, reducing the risk of manipulated IoCs. This approach also minimizes compute spend since hashing is lightweight compared to continuous verification processes.

Therefore, the strongest alignment with all stated objectives”availability, reduced spend, reduced attack surface, and integrity”is achieved by providing hashes of all threat intelligence data.

QUESTION 268

A SOC analyst is investigating an event in which a penetration tester was able to successfully create and execute a payload. The analyst pulls the following command history from the affected server-

```
$ uname -a && env
$ vim foo.c
$ gcc foo.c /tmp/lockfile
$ chmod +x /tmp/lockfile
$ ./tmp/lockfile
```

Which of the following should the analyst implement lo improve the security of the server?

A. Kernel-supported ASLR controls

B. Application controls with allow lists

C. OS restrictions of globally writable folders

Answer: D. EDR signatures that terminate specific processes B

The best way to mitigate the ability of attackers or penetration testers to execute arbitrary payloads

is to enforce application controls with allow lists (B). Application allow listing ensures that only preapproved, trusted software and scripts can be executed on the system. This prevents attackers from

dropping or running malicious binaries, even if they exploit vulnerabilities to gain access. CAS-005 emphasizes allow listing as a preventive control against post-exploitation persistence and lateral movement.

Option A (ASLR) randomizes memory addresses and helps mitigate buffer overflow exploits but does not directly prevent execution of unauthorized programs. Option C (OS restrictions of globally writable folders) improves security hygiene but still does not stop attackers from executing already placed payloads in non-restricted locations. Option D (EDR signatures) are reactive and limited, since

QUESTION 269

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

Answer: D. Endpoint detection A

The correct answer is Playbooks (A). In incident response, playbooks are structured workflows that define step-by-step actions for specific incident types (e.g., ransomware, phishing, insider threats). They allow SOC analysts to standardize responses across multiple platforms and tools, ensuring consistency and faster mitigation. By leveraging playbooks, organizations integrate existing incident response tools into automated or semi-automated processes, improving efficiency and reducing human error.

Option B (event collectors) consolidate logs but do not directly improve response processes. Option C (centralized logging) enhances visibility but does not provide a framework for action. Option D (endpoint detection) expands detection capabilities but does not enhance the process effectiveness

of incident response.

CAS-005 emphasizes structured response through automation and orchestration. Playbooks, often implemented via SOAR platforms, allow integration of detection, triage, and remediation steps, making them the most effective way to increase incident response maturity.

QUESTION 270

A company notices that cloud environment costs increased after using a new serverless solution based on API requests. Many invalid requests from unknown IPs were found, often within a short time. Which of the following solutions would most likely solve this issue, reduce cost, and improve security?

A. Using digital certificates for known customers and performing API authorization through those certificates

B. Defining request rate limits and comparing new requests from unknown IPs with a list of knownmalicious

C. Setting authentication processes for the API requests as well as proper rate limits according to regular usage

Answer: D. Only allowing API requests coming from regions with known customers C

The best solution is to implement authentication for API requests and apply appropriate rate limiting

(C). Authentication ensures that only authorized customers or systems can access the API, while rate limiting helps prevent denial-of-service (DoS)-like conditions and cost inflation from excessive or malicious requests. This addresses both the security (unauthorized access) and cost issues (serverless billing based on execution).

Option A (digital certificates) is a strong control for authentication but may introduce unnecessary complexity and does not address rate abuse directly. Option B (rate limits with IP reputation checks) is useful but insufficient”malicious actors may rotate through new IPs not yet flagged. Option D (regional restrictions) might reduce some noise traffic but risks blocking legitimate global users and is not scalable for a modern cloud service.

CAS-005 highlights securing APIs with authentication, authorization, and throttling as best practices. Thus, the combined approach of API authentication plus rate limiting is the most comprehensive and effective solution.

QUESTION 271

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: D

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, corporateapproved 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

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.

QUESTION 272

A manufacturing plant is updating its IT services. During discussions, the senior management team created the following list of considerations:

Staff turnover is high and seasonal.

Extreme conditions often damage endpoints. Losses from downtime must be minimized. Regulatory data retention requirements exist.

Which of the following best addresses the considerations?

A. Establishing further environmental controls to limit equipment damage

B. Using a non-persistent virtual desktop interface with thin clients

C. Deploying redundant file servers and configuring database journaling

Answer: D. Maintaining an inventory of spare endpoints for rapid deployment B

The best solution is to use a non-persistent virtual desktop infrastructure (VDI) with thin clients (B). Thin clients are inexpensive, easy to replace, and resilient in harsh environments where traditional endpoints may be damaged. With non-persistent VDI, employee desktops are virtualized and reset to a clean state after logout, reducing risks from turnover, malware persistence, or user misconfiguration. Centralized management ensures consistent patching and security updates while minimizing downtime, since damaged thin clients can be swapped quickly with minimal disruption. Option A (environmental controls) may reduce equipment damage but does not address turnover or regulatory retention requirements. Option C (redundant servers and journaling) improves data integrity but does not solve endpoint-related risks or staffing issues. Option D (maintaining spare endpoints) mitigates hardware failures but still relies on managing and configuring full systems, which is inefficient for high-turnover environments.

CAS-005 emphasizes virtualization and centralization strategies in environments where operational resilience, rapid recovery, and compliance are critical. Non-persistent VDI with thin clients provides the most comprehensive solution here.

QUESTION 273

Engineers at a cloud service provider can now access newly deployed customer environments from their personal laptops. The engineers are concerned that unmanaged systems may present unknown

A. Modifying MDM policies to provide device attestation on all devices connecting to the cloud service's management console

B. Requiring that a corporate-licensed and -managed EDR solution is installed on employee-owned laptops

C. Configuring the device's certificate-based authentication on the corporate VPN and requiring that all activity in customer environments be performed using the VPN

D. Implementing host checking on remote desktop sessions to jump boxes used for managing customer environments

Answer: B

The best way to reduce liability and secure customer environments is to require that all employeeowned laptops have a corporate-licensed and managed Endpoint Detection and Response (EDR)

solution installed. This ensures that devices accessing sensitive customer infrastructure are monitored for malware, unauthorized processes, and suspicious behaviors. EDR provides visibility into endpoint security posture and enforces corporate security baselines, which unmanaged personal devices typically lack.

Option A (MDM with attestation) works well for corporate-owned devices but is difficult to enforce reliably across personally owned laptops. Option C (VPN with certificate authentication) ensures encrypted access but does not validate whether the device is secure. Option D (host checking to jump boxes) reduces exposure but still allows unmanaged endpoints to connect indirectly.

CAS-005 emphasizes endpoint controls and assurance mechanisms for environments with third-party

or bring-your-own-device (BYOD) risk. Deploying managed EDR ensures visibility, consistent policies, and rapid response across all devices, making this the most secure and practical option.

QUESTION 274

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

The correct source is the Business Impact Analysis (BIA). A BIA provides context about which systems and applications are most critical to business operations, regulatory compliance, and customer obligations. While CVSS scores indicate severity in technical terms, they do not reflect the business impact of exploitation. For example, a medium-severity vulnerability on a critical payment system

may pose more business risk than a high-severity vulnerability on a test server.

Option A (third-party risk review) focuses on vendor security posture, not internal remediation priorities. Option C (incident response playbook) guides response during active incidents, not vulnerability prioritization. Option D (crisis management plan) addresses executive-level communications during crises, not technical risk assessment.

By combining vulnerability scan data with BIA context, security teams can prioritize remediation efforts based on business-critical systems, ensuring the highest-risk vulnerabilities are remediated first. This aligns with CAS-005s guidance on risk-based prioritization of remediation efforts.

QUESTION 275

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:

```
21487592579325342038509345083453432452523435235345523453243534245234534523453896276563857932578395378543620382630532804508325
```

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

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,

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.

QUESTION 276

A company's Chief Information Security Officer learns that the senior leadership team is traveling to a country accused of attempting to steal intellectual property saved on laptops. Which of the following is the best method to protect against this attack?

A. Configure Measured Boot to report any firmware changes.

B. Use sanitized devices with remote connections to VDI.

C. Deploy self-encrypting drives to protect company data.

D. Install tamper-evident stickers over any laptop screws.

Answer: B

The best option is to provide sanitized devices with remote connections to a Virtual Desktop Infrastructure (VDI). This ensures that no sensitive intellectual property is stored locally on the laptops carried across borders. Even if the devices are inspected, seized, or tampered with, attackers cannot access corporate data since all sensitive files remain within secure, centralized infrastructure. Option A (Measured Boot) reports firmware tampering but does not prevent data theft if the device is compromised. Option C (self-encrypting drives) protect data at rest but can be bypassed if customs

agents demand login credentials. Option D (tamper-evident stickers) provide only physical inspection indicators and are ineffective against sophisticated data theft attempts.

CAS-005 emphasizes secure remote access strategies and temporary œclean laptops for high-risk travel scenarios. Sanitized laptops with VDI access minimize exposure while maintaining productivity, making this the strongest mitigation.

QUESTION 277

An organization is developing an in-house software platform to support capital planning and reporting functions. In addition to role-based access controls and auditing/logging capabilities, the product manager must include requirements associated with archiving data and immutable backups. Which of the following organizational considerations are most likely associated with this requirement? (Select two)

B. Supply chain weaknesses

C. Device attestation

D. Quality assurance

E. Legal hold compliance

F. Ransomware resilience

Answer: E,F

The requirements for archiving data and immutable backups directly align with legal hold compliance

(E) and ransomware resilience (F).

Legal hold compliance ensures that organizations can retain data in a tamper-proof manner when required for litigation, regulatory mandates, or audits. Immutable backups satisfy this by preventing unauthorized changes or deletion, ensuring evidence and records are preserved.

Ransomware resilience is also a key factor. Immutable backups allow recovery from ransomware attacks, as attackers cannot encrypt or delete data stored in read-only or write-once media. This reduces downtime and supports business continuity.

Options A (crypto-export), B (supply chain), C (device attestation), and D (quality assurance) do not relate directly to data archiving or immutable storage.

CAS-005 stresses aligning security controls with business continuity and compliance requirements. By focusing on legal and ransomware-related considerations, the organization ensures both regulatory and operational resilience.

QUESTION 278

Consultants for a company learn that customs agents at foreign border crossings are demanding device inspections. The company wants to:

Minimize the risk to its data by storing its most sensitive data inside of a security container. Obfuscate containerized data on command.

Which of the following technologies is the best way to accomplish this goal?

A. SED

B. eFuse

C. UEFI

D. vTPM

Answer: E. MicroSD HSM A

The best solution is to use Self-Encrypting Drives (SEDs). SEDs automatically encrypt all data stored on the disk and can be rapidly sanitized or obfuscated by deleting or altering the encryption keys.

Option B (eFuse) and C (UEFI) are hardware mechanisms unrelated to dynamic data protection. Option D (vTPM) provides virtualized key storage but does not obfuscate data quickly under inspection conditions. Option E (MicroSD HSM) is useful for key storage but does not protect all data at scale.

CAS-005 highlights hardware-based encryption solutions like SEDs for protecting sensitive data during travel, ensuring both regulatory compliance and rapid response capabilities under hostile conditions.

QUESTION 279

A security manager at a local hospital wants to secure patient medical records. The manager needs to:

Choose an access control model that clearly defines who has access to sensitive information. Prevent those who enter new patient information from specifying who has access to this data. Which of the following access control models is the best way to ensure the lowest risk of granting unintentional access?

A. Rule-based

B. Attribute-based

C. Mandatory

D. Discretionary

Answer: C

The best option is Mandatory Access Control (MAC). In MAC, access decisions are centrally controlled by the system or administrators, not by individual users. This ensures that healthcare staff who enter patient information cannot grant access to others, thereby preventing accidental or malicious

disclosure. MAC enforces strict policies based on data sensitivity and user clearance, which aligns with compliance requirements like HIPAA.

Option A (rule-based) defines access through specific rules but is not as rigidly enforced as MAC. Option B (attribute-based) is flexible but could still allow dynamic grants of access. Option D (discretionary) explicitly allows users to assign access rights, which is exactly what must be avoided in this scenario.

CAS-005 stresses using centralized, non-discretionary controls when protecting sensitive medical data, making MAC the correct choice for hospitals.

QUESTION 280

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

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

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.

Anns 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.

QUESTION 281

A security administrator needs to review the efficacy of the detection rules configured on the SIEM by employing real-world attacker TTPs. Which of the following actions should the security administrator take to accomplish this objective?

A. Perform an internal penetration test.

C. Execute an internal vulnerability assessment.

D. Perform a threat hunt exercise.

E. Ingest new threat intelligence feeds.

Answer: B

The best option is adversary emulation. Adversary emulation involves simulating real-world attacker Tactics, Techniques, and Procedures (TTPs) based on frameworks like MITRE ATT&CK. Unlike penetration tests, which primarily focus on identifying exploitable vulnerabilities, adversary emulation specifically tests the effectiveness of detection and response capabilities against known adversarial behaviors.

Option A (penetration testing) provides value but may not align test cases with SIEM detection rules. Option C (vulnerability assessment) identifies weaknesses but does not test detection rules. Option D (threat hunting) is proactive analysis but does not validate existing SIEM rule coverage in a structured manner. Option E (threat feeds) enrich SIEM data but do not test its efficacy.

CAS-005 identifies adversary emulation as a key strategy for validating detection and response coverage. It provides measurable results about what alerts are triggered and where detection gaps exist, enabling organizations to tune SIEM rules for improved efficacy.

QUESTION 282

A game developer wants to reach new markets and is advised by legal counsel to include specific age-related sign-up requirements. Which of the following best describes the legal counsel's concerns?

A. GDPR

B. LGPD

C. PCI DSS

D. COPPA

Answer: D

The correct regulation is COPPA (Childrens Online Privacy Protection Act). COPPA is a U.S. law that requires organizations to obtain parental consent and implement specific protections before

collecting personal data from children under the age of 13. Since the legal counsel is advising about age-related sign-up requirements, the concern clearly points to COPPA compliance.

GDPR (A) is a European regulation governing privacy and data protection but is broader and not specifically tied to childrens age verification, though it has related provisions. LGPD (B) is Brazils data protection law, similar in scope to GDPR. PCI DSS (C) is focused on protecting cardholder data in payment environments, unrelated to age-related concerns.

QUESTION 283

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?

A. name: deployment hosts: linux_servers remote_user: root tasks: - name: Install security

software ansible.builtin.apt:

B. linux_servers Linux 3.1 true

com.canonical.io

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

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

Answer: A

The correct snippet is Option A, which shows an Ansible YAML playbook designed to deploy and maintain security software on Linux servers. Ansible is a configuration management tool widely used in enterprise environments, and the ansible.builtin.apt module specifically manages package installation on Debian/Ubuntu-based Linux distributions. This ensures consistent security software deployment across multiple servers.

Option B is XML-based and does not represent a valid configuration management script. Option C incorrectly uses JSON format and references Microsofts store (com.microsoft.store.latest), which is irrelevant for Linux. Option D also uses JSON syntax with œAppX, which applies to Windows applications, not Linux.

CAS-005 emphasizes infrastructure as code (IaC) and automation as best practices for secure system configuration. YAML-based playbooks in Ansible provide repeatability, auditability, and scalability, making Option A the most secure and appropriate solution.

QUESTION 284

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:

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

A. Consulting logs from the enterprise password manager

B. Searching dark web monitoring resources for exposure

C. Reviewing audit logs from privileged actions

Answer: D. Querying user behavior analytics data D

The best step is to query user behavior analytics (UBA) data. SIEM alerts provide potential security events, but without additional context, they may lead to false positives. UBA solutions detect anomalies by comparing user activity against baselines of normal behavior, highlighting unusual login patterns, lateral movement, or privilege escalation.

Option A (password manager logs) focuses only on credential use and lacks behavioral insight. Option B (dark web monitoring) helps identify compromised accounts but does not investigate the internal incident. Option C (audit logs for privileged actions) is useful but narrow in scope”it only covers administrator accounts.

By correlating SIEM data with UBA, the engineer can validate whether the flagged activity indicates real malicious behavior or benign anomalies. CAS-005 emphasizes advanced analytics integration (UEBA/UBA) to strengthen investigation and reduce false positives, making Option D the most effective choice.

QUESTION 285

A security analyst is developing a threat model that focuses on attacks associated with the organization's storage products. The products:

Are used in commercial and government user environments Are required to comply with crypto-export requirements

Include both hardware and software components that are developed by external vendors in Europe and Asia

Which of the following are the most important for the analyst to consider when developing the model? (Select two).

B. Legal hold obligations

C. Trust boundaries

D. Cloud services enumeration

E. Supply chain access

Answer: F. Homomorphic encryption usage C,E

The most critical considerations are trust boundaries (C) and supply chain access (E). Trust boundaries define where sensitive data crosses between systems or organizations, requiring strict cryptographic protections”especially important in government and commercial environments subject to crypto-export controls.

Supply chain access is also critical because hardware and software are sourced from external vendors. If suppliers are compromised, attackers could introduce malicious code, backdoors, or tampered firmware, endangering customers worldwide.

Option A (contractual obligations) and B (legal hold) are compliance-related but not direct security threats. Option D (cloud services enumeration) is irrelevant unless the storage is cloud-based. Option F (homomorphic encryption) is an advanced technology but not required for base threat modeling.

CAS-005 highlights modeling adversary capabilities at trust boundaries and accounting for supply chain risks, making C and E the most important.

QUESTION 286

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

Answer: D. Deploy OpenID Connect for API authentication A

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

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.

QUESTION 287

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

Answer: D. Using the best practices in the OWASP secure coding manual to define a new roadmap A

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 organizations 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.

QUESTION 288

An organization is increasing its focus on training that addresses new social engineering and phishing attacks. Which of the following is the organization most concerned about?

A. Meeting existing regulatory compliance

B. Overreliance on AI support bots

C. Generative AI tools increasing the quality of exploits

D. Differential analysis using AI models

Answer: C

The organization is most concerned about Generative AI improving phishing and social engineering attacks. Tools like ChatGPT can generate highly convincing phishing emails, fake websites, and human-like interactions that bypass traditional detection methods. Employees who were trained to spot poor grammar or obvious scams may now struggle to detect AI-crafted exploits.

Option A relates to compliance but not AI-driven threats. Option B (overreliance on AI bots) is operational risk, not phishing. Option D (differential analysis) applies to AI privacy issues, not phishing.

CAS-005 emphasizes adapting training to emerging threats, including AI-enabled social engineering. This ensures users remain resilient against modern attacks, making C the correct answer.

QUESTION 289

A company sells a security appliance assembled from globally sourced hardware and software components. Installing the security appliance requires enabling administrative permissions for the service accounts on the appliance. Which of the following allows the company to reassure new and existing customers that the risk introduced by the appliance is minimal?

A. The results of a qualitative risk analysis performed on the appliance

B. A business impact analysis and risk prioritization process

C. Results of internal risk reduction studies conducted by a third-party assessor

Answer: D. A transparent supply chain risk management and testing program D

QUESTION 290

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. Dark web monitoring

B. Adversary emulation engagement

C. Supply chain risk consultation

D. Tabletop exercises

Answer: B

QUESTION 291

A company wants to perform threat modeling on an internally developed, business-critical application. The Chief Information Security Officer (CISO) is most concerned that the application should maintain 99.999% availability and authorized users should only be able to gain access to data they are explicitly authorized to view. Which of the following threat-modeling frameworks directly addresses the CISO's concerns about this system?

A. CAPEC

B. STRIDE

C. ATT&CK

D. TAXII

Answer: B

QUESTION 292

An organization is deploying a new data lake that will centralize records from several applications. During the design phase, the security architect identifies the following requirements:

The sensitivity levels of the data is different.

The data must be accessed through stateless API calls after authentication. Different users will have access to different data sets.

Which of the following should the architect implement to best meet these requirements?

A. Directory services

B. 802.1X with EAP-TLS

C. OpenID Connect

D. CASB

Answer: C

QUESTION 293

While investigating an email server that crashed, an analyst reviews the following log files:

Which of the following is most likely the root cause?

A. The administrator's account credentials were intercepted and reused.

B. The backup process did not complete and caused cascading failure.

C. A hardware failure in the storage array caused the mailboxes to be inaccessible.

D. A user with low privileges was able to escalate and erase all mailboxes.

Answer: D

QUESTION 294

A security engineer needs to create multiple servers in a company's private cloud. The servers should have a virtual network infrastructure that supports connectivity, as well as security configurations applied using predefined templates. Which of the following is the best option for the security engineer to consider for the deployment?

A. Installing a container orchestration solution locally, configuring the infrastructure, and cloning the solution

B. Creating templates on the cloud provider marketplace and modeling the solution using those templates

C. Using Terraform to implement an infrastructure as code model with the existing private cloud solution

Answer: D. Integrating the cloud provider API to the CI/CD pipeline model used by the company C

QUESTION 295

An engineer wants to automate several tasks by running commands daily on a UNIX server. The engineer has only built-in, default tools available. Which of the following should the engineer use to best assist with this effort? (Select Two).

B. Cron

C. Ansible

D. PowerShell

E. Bash

Answer: F. Task Scheduler B,E

QUESTION 296

A development team must create a website to share indicators of compromise. The team wants to use APIs between industry peers to aid in configuring SIEM and SOAR. The team needs to create a free tier of service, and the senior developer insists on configuring rate limiting. Which of the following best describes the senior developer's reasoning?

A. To prevent password-spraying attacks on the services hosting the API

B. To limit the likelihood of resource exhaustion occurring on the API server

C. To address concerns the team has about API bandwidth utilization

Answer: D. To reduce attack surface exposure of the API endpoints connecting peers B

QUESTION 297

Emails that the marketing department is sending to customers are going to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three).

A. DMARC

B. SPF

C. DKIM

D. DNSSEC

E. SASE

F. SAN

G. SOA

H. MX

Answer: A,B,C

QUESTION 298

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. Configure a reverse proxy to protect the data.

B. Implement an on-demand VPN connection.

C. Deploy an API gateway protected with access tokens.

Answer: D. Continually publish all relevant data to a CDN. C

QUESTION 299

While performing threat-hunting functions, an analyst is using the Diamond Model of Intrusion Analysis. The analyst identifies the likely adversary, the infrastructure involved, and the target. Which of the following must the threat hunter document to use the model effectively?

A. Knowledge

B. Capabilities

C. Phase

Answer: D. Methodologies B

QUESTION 300

A security architect is troubleshooting an issue with an OIDC implementation. The architect reviews the following configuration and errors:

Error: Invalid authentication request code

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

A. The redirect-url parameter is not in the allowed list of redirect hosts in the configuration.

B. Introspection is not enabled within the OIDC code implementation.

C. The encoding of the URL parameters on the proxy system is failing.

D. The state parameter is being reused within the authentication challenge.

E. OAuth 2.0 was unable to verify the lack of an interception attack.

Answer: A

QUESTION 301

A company must meet the following security requirements when implementing controls in order to be compliant with government policy:

Access to the system document repository must be MFA enabled. Ongoing risk monitoring must be displayed on a system dashboard. Staff must receive email notifications about periodic tasks.

Which of the following best meets all of these requirements?

A. Implementing a GRC tool

B. Configuring a privileged access management system

C. Launching a vulnerability management program

Answer: D. Creating a risk register A

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

Answer: D. Collecting operational system logs and storage disk data D

QUESTION 303

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 enable log correlation using machine learning

C. To orchestrate additional reporting for the security operations center

Answer: D. To prepare runbooks to automate future incident response D

QUESTION 304

A company developed a new solution that needs to track any changes to the data, and the changes need to be quickly identified. If any changes are attempted without prior approval, multiple events must be triggered, such as:

Raising alerts

Blocking the unapproved changes Quickly removing access to the data

Which of the following solutions best meets these requirements?

A. Tracking all application logs, integrating them to the existing SIEM, flagging any changes, and

B. Implementing a file integrity monitoring tool and integrating it via orchestration and automation with other security tools

C. Introducing more granular access controls and allowing read-only access for non-privileged users

Answer: D. Configuring CASB rules, making access to the data available only to authorized personnel B

QUESTION 305

A security analyst is performing threat modeling for a new AI chatbot. The AI chatbot will be rolled out to help customers develop configuration information within the company's SaaS offering. Which of the following issues would require involvement from the company's internal legal team?

A. An internal user finds a way to use prompt injection to disregard guardrails.

B. A DoS vulnerability exists that could impact all customers who use the chatbot.

C. A bug bounty of an exploitable model inversion vulnerability is submitted.

D. User consent is not being collected before training models on customer data.

E. An access control issue is allowing the model to be poisoned with incorrect information.

Answer: D

QUESTION 306

Which of the following most likely explains the reason a security engineer replaced ECC with a lattice-based cryptographic technique?

A. It is computationally efficient and provides perfect forward secrecy.

B. It is more resilient to brute-force attacks than ECC.

C. It supports ephemeral key exchange and digital signatures.

D. It is currently considered a robust PQC technique.

E. It enables processing on data while remaining in an encrypted state.

Answer: D

QUESTION 307

A cybersecurity architect seeks to improve vulnerability management and orchestrate a large number of vulnerability checks. Key constraints include:

. Vulnerability data is sourced from multiple scanners.

. CIS baselines must be enforced.

. Scan activity must be scheduled.

Which of the following automation workflows best meets this objective?

A. Employing an endpoint data collection system

B. Deploying an XCCDF scanner

C. Utilizing CVSS reports for SOC analysts

Answer: D. Using a repository scanner to enforce IaC security B

QUESTION 308

A company implements an AI model that handles sensitive and personally identifiable information. Which of the following threats is most likely the company's primary concern?

A. Unsecured output handling

B. Model theft

C. Model poisoning

Answer: D. Prompt injection A

QUESTION 309

An organization recently experienced a security incident due to an exterior door in a busy area getting stuck open. The organization launches a security campaign focused on the motto, "See Something, Say Something." Which of the following best describes what the organization wants to educate employees about?

A. Situational awareness

B. Phishing

C. Social engineering

Answer: D. Tailgating A

An incident response analyst finds the following content inside of a log file that was collected from a compromised server:

.2308464678 ... whoami ..... su2032829%72%322/// ..... /etc/passwd .... 2087031731467478432 ...

$6490/./ ..< XML ? nty.

Which of the following is the best action to prevent future compromise?

A. Blocking the processing of external files by forwarding them to another server for processing

B. Implementing an allow list for all text boxes throughout the web application

C. Filtering inserted characters for all user inputs and allowing only ASCII characters

Answer: D. Improving file-parsing capabilities to stop external entities from executing commands D

QUESTION 311

An application requires the storage of PII. A systems engineer needs to implement a solution that uses an external device for key management. Which of the following is the best solution?

A. TPM

B. SBoM

C. vTPM

D. HSM

Answer: D

QUESTION 312

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_CCM_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?

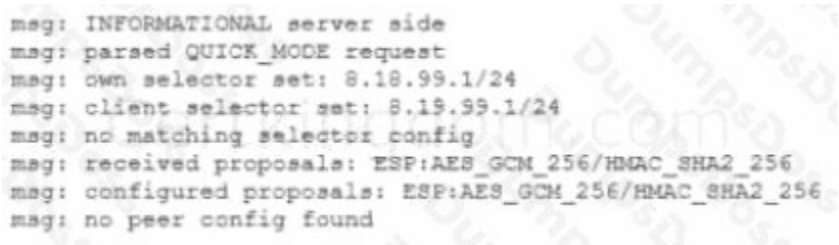
A. Removing any ciphers utilizing cipher block chaining

C. Deploying a WAF to monitor web traffic

Answer: D. Reissuing new SSL certificates for the website A

QUESTION 313

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



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

A. Enable perfect forward secrecy on the remote peer.

B. Update the cipher suites configured for use on the server side.

C. Add a new subnet as a permitted initiator.

D. Disable IKE version 1 and run IKE version 2.

Answer: C

QUESTION 314

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? (Select Two.)

A. EDR

B. HIDS

C. Web application firewall

E. Host-based firewall

F. TPM

Answer: A,D

QUESTION 315

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: <sdflkh038-kdhen7-23hd7s-afdzx.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

QUESTION 316

A security operations analyst is reviewing network traffic baselines for nightly database backups. Given the following information:

Which of the following should the security analyst do next?

A. Consult with a network engineer to determine the impact of bandwidth usage

B. Quarantine PRDDB01 and then alert the database engineers

C. Refer to the incident response playbook for the proper response

Answer: D. Review all the network logs for further data exfiltration D

QUESTION 317

An organization wants to implement a secure cloud architecture across all instances. Given the following requirements:

Â· Establish a standard network template. Â· Deployments must be consistent.

Â· Security policies must be able to be changed at scale. Which of the following technologies meets these requirements?

A. Serverless deployment model

B. Container orchestration

C. Infrastructure as code

D. CLI cloud administration

Answer: E. API gateway C

QUESTION 318

A security engineer needs to remediate a SWEET32 vulnerability in an OpenSSH-based application and review existing configurations. Which of the following should the security engineer do? (Select two.)

A. Disable Twofish algorithms

C. Disable RSA algorithms

D. cat /etc/sshd/ssh_config | grep "PermitRootLogin"

E. Disable 3DES algorithms

Answer: F. cat /etc/sshd/ssh_config | grep "Ciphers" E,F

QUESTION 319

Which of the following are the best ways to mitigate the threats that are the highest priority? (Select two).

A. Isolate network systems using Zero Trust architecture with microsegmentation and SD-WAN

B. Scan all systems and source code with access to sensitive data for vulnerabilities.

C. Implement a cloud access security broker and place it in blocking mode to prevent information exfiltration.

D. Apply data labeling to all sensitive information within the environment with special attention to payroll information.

E. Institute a technical approval process that requires multiple parties to sign off on mass payroll changes.

Answer: A,E

QUESTION 320

During a security review for the CI/CD process, a security engineer discovers the following information in a testing repository from the company:

Which of the following options is the best countermeasure to prevent this issue in the future?

A. Performing an application penetration test over the testing environment before moving to production

B. Changing the repository technology to avoid inclusion of confidential information

C. Automating the upload process of code to the repository and improving the software development life cycle

Answer: D. Using a secrets management platform to share and manage confidential information D

QUESTION 321

In order to follow new regulations, the Chief Information Security Officer plans to use a defense-indepth approach for a perimeter network. Which of the following protections would best achieve this

goal?

A. SAST, DAST, IAST

B. NGFW, IPS, EDR

C. SASE, IDS, SAST

D. CASB, DLP, EDR

Answer: B

QUESTION 322

A security engineer wants to enhance the security posture of end-user systems in a Zero Trust

. Reduce the ability for potentially compromised endpoints to contact command-and-control 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. DNS sinkholing

B. Browser isolation

C. Zone transfer protection

D. HIDS

Answer: A

QUESTION 323

A nation-state actor is exposed for attacking large corporations by establishing persistence in smaller companies that are likely to be acquired by these large corporations. The actor then provisions user accounts in the companies for use post-acquisition. Before an upcoming acquisition, a security officer conducts threat modeling with this attack vector. Which of the following practices is the best way to investigate this threat?

A. Restricting internet traffic originating from countries in which the nation-state actor is known to operate

B. Comparing all existing credentials to personnel and services

C. Auditing vendors to mitigate supply chain risk during the acquisition

Answer: D. Placing a hold on all information about corporate interest in acquisitions B

QUESTION 324

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

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 removable storage.

Answer: B

QUESTION 325

A developer receives feedback about code quality and efficiency. The developer needs to identify and resolve the following coding issues before submitting the code changes for peer review: Indexing beyond arrays

Dereferencing null pointers

Potentially dangerous data type combinations Unreachable code

Non-portable constructs

Which of the following would be most appropriate for the developer to use in this situation?

A. Linting

B. SBoM

C. DAST

D. Branch protection

Answer: E. Software composition analysis A

QUESTION 326

A company plans to deploy a new online application that provides video training for its customers. As part of the design, the application must be:

Fast for all users

Available for users worldwide Protected against attacks

Which of the following are the best components the company should use to meet these requirements? (Select two).

B. IPS

C. CDN

D. SASE

E. VPN

F. CASB

Answer: A,C

QUESTION 327

A penetration tester is drafting a report of findings and recommendations. Multiple EOL biomedical devices were compromised using a combination of known-exploit payloads for CVEs and VLAN hopping. The tester acknowledges that the systems cannot be changed or replaced in the hospital

due to regulatory, safety, and cost reasons. Which of the following are the most effective controls for this scenario? (Select two).

A. Deploying an IDS with active response for threat activities from a network tap

B. Implementing QoS that limits the throughput of the link speeds from some VLANs

C. Limiting trunking protocols to specific uplink ports of access switches

D. Adding a proxy and requiring medical staff to authenticate every connection

E. Inserting an in-line IPS between network segments of the affected hosts

Answer: F. Performing security awareness training for these device users C, E

The best two controls are C and E because the scenario has two distinct technical problems: the biomedical devices are EOL and vulnerable to known CVEs, and

the attacker also used VLAN hopping.

Since the devices cannot be patched, replaced, or materially changed, the strongest response is to apply compensating network controls around them. That makes this primarily a Security Architecture question focused on segmentation and preventive controls. CompTIAs official SecurityX CAS-005 objectives explicitly include œNetwork architecture: segmentation, microsegmentation¦ and also list œproactive, detective, and preventative controls as part of control strategy design.

Why C is correct:

Limiting trunking protocols to specific uplink ports of access switches directly addresses the VLAN hopping portion of the attack. VLAN hopping commonly succeeds when switch ports are incorrectly allowed to negotiate or carry trunk traffic where they should function only as access ports.

Restricting trunking to designated uplinks reduces the chance that an attacker can pivot between

Why E is correct:

Inserting an in-line IPS between network segments of the affected hosts is the strongest compensating control for the known CVE exploit traffic against EOL devices. Because the systems cannot be updated, an in-line IPS can actively inspect and block malicious payloads moving between segments. This is much more effective than passive monitoring alone because it is a preventive control, not just a detective one. CompTIAs official SecurityX objectives specifically emphasize preventative controls and segmentation/microsegmentation, which is exactly what this design uses

to protect unpatchable assets.

Why the other options are not the best answers:

A . IDS with active response from a network tap is weaker than an in-line IPS in this case. A network

tap is out-of-band, so detection may help visibility, but it does not provide the same direct trafficblocking capability as an in-line preventive control. In a hospital with unpatchable biomedical

systems, prevention at segmentation boundaries is more effective than relying mainly on monitoring. CompTIAs objectives distinguish between detective and preventative controls, and this scenario clearly favors prevention.

B . QoS limiting throughput does not address either root cause. Lower bandwidth does not stop CVE exploitation and does not prevent VLAN hopping. It may reduce traffic volume, but it is not a meaningful security mitigation for the attack described.

D . Adding a proxy and requiring staff authentication every connection is not the most effective answer because the compromise described is tied to device vulnerabilities and network segmentation weaknesses, not primarily to user authentication. It also may be operationally unsuitable for biomedical workflows.

F . Security awareness training is valuable in general, but it is not an effective primary control for exploit payloads against EOL medical devices or VLAN hopping. The problem is architectural and technical, so the answer must also be architectural and technical.

Official extract alignment:

A short official extract from CompTIAs SecurityX CAS-005 objectives summary that supports this answer is: œNetwork architecture: segmentation, microsegmentation¦ and œCloud control strategies: proactive, detective, and preventative controls¦ . Also, in CompTIAs official SecurityX practice questions, CompTIA gives a related design pattern for constrained/embedded devices: œOperating IoT devices on a separate network with no access to other devices internally , which reinforces isolation and segmentation as the preferred control approach for hard-to-modify devices. Reference:

CompTIA SecurityX (CAS-005) official certification page and exam objectives summary.

CompTIA SecurityX (V5) official practice questions, especially the separate-network control example for IoT devices.

QUESTION 328

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

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

Answer: D. Deploying a proxy server at the manufacturing plant B

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 companys security posture. In

CompTIA SecurityX CAS-005, SD-WAN is explicitly part of Security Architecture, under œDeperimeterization: SASE, SD-WAN, and software-defined networking. The same official objective set also lists œNetwork architecture: segmentation, microsegmentation, VPN¦ and œSecurity 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 CompTIAs 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, œpatching 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-tosite 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.

Reference:

CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, especially Security Architecture domains covering SD-WAN, segmentation, VPN, and secure zones.

==========

QUESTION 329

A government agency implements a configuration that disables cellular network access on government-issued devices while roaming internationally. The agency issues mobile hot-spots and

A. To protect against SIM hijack vulnerabilities

B. To defend from carrier OTA attack vectors

C. To block malicious radio connections

D. To prevent attempts to downgrade the protocol to legacy 3G

Answer: E. To filter directed electromagnetic interference C

The best answer is C. To block malicious radio connections. The agency is preventing the government-issued endpoint itself from directly attaching to foreign cellular networks while roaming. That reduces the exposure of the endpoint to hostile or untrusted cellular infrastructure, including rogue or malicious radio environments. Requiring the use of agency-issued hotspots keeps the endpoint off direct cellular attachment and places the radio exposure on a controlled intermediary device instead. In CompTIA SecurityX CAS-005, one of the core expected skills is to œutilize cryptographic technologies and techniques while evaluating the impact of emerging trends¦ on information security and to design secure solutions across complex environments. This question fits that theme of managing risk from modern communications technologies through architecture

and control choices.

Why the other options are less accurate:

A is too specific because the scenario is broader than SIM hijacking; disabling direct cellular service on the endpoint is not solely about SIM theft. B is less accurate because the hotspot still depends on

a carrier, so this does not fully eliminate over-the-air carrier-related risks. D is possible as a radiosecurity concern, but the question is framed more broadly around disallowing direct endpoint

cellular connections altogether, so malicious radio connections is the more complete rationale. E is incorrect because directed electromagnetic interference is not what mobile hotspots are primarily designed to mitigate in this context.

Reference:

CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, including secure solution design across complex environments and evaluating emerging technology impacts on security.

==========

QUESTION 330

A developer receives feedback about code quality and efficiency. The developer needs to identify and resolve the following coding issues before submitting the code changes for peer review: Indexing beyond arrays

Dereferencing null pointers

Potentially dangerous data type combinations

Non-portable constructs

Which of the following would be most appropriate for the developer to use in this situation?

A. Linting

B. SBoM

C. DAST

D. Branch protection

Answer: E. Software composition analysis A

The best answer is

A. Linting. The listed problems are classic source-code quality and static-analysis

findings: out-of-bounds array indexing, null dereferences, unsafe type use, unreachable code, and non-portable constructs. A linter is designed to inspect code before execution and flag these classes

of issues early in the development workflow. In the official CompTIA SecurityX CAS-005 objectives, Security Engineering includes œAutomation: scripting¦ workflow automation and broader secure engineering practices. Using a linter fits that model because it is an automated developer-side

control that improves code quality before peer review and release. Why the other options are not correct:

B. SBoM documents software components and dependencies; it does not primarily detect unreachable code or null dereferences in custom source code. C. DAST tests a running application from the outside and is not the best tool for finding these code-level static issues before peer review.

D. Branch protection is a repository control for workflow governance, not a code-analysis mechanism. E. Software composition analysis focuses mainly on third-party libraries, dependency risk, licensing, and known vulnerabilities in components, not on first-party code defects like array bounds and unreachable code.

Reference:

CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, especially the Security Engineering domain and its emphasis on automation and secure engineering practices.

QUESTION 331

A penetration tester reviews the following router configuration: set-system services ssh root login-allow

set-system services web-management https allow set-system services syslog file interactive

set-system services log mode stream

set-interfaces 0 family inet address 10.12.14.1

Which of the following changes is the best way to enhance security?

B. Disabling access to unencrypted terminal connections

C. Enabling network segmentation controls

Answer: D. Configuring automatic patching and rebooting of the device C

The best answer is C. Enabling network segmentation controls. The most obvious security weakness shown in the configuration is the interface address 10.12.14.1, which places the device in an extremely broad network range instead of a

tightly bounded segment. From a SecurityX perspective, the strongest improvement is to reduce unnecessary trust exposure by applying segmentation and tighter network boundaries. CompTIAs official SecurityX objectives explicitly call out œNetwork architecture: segmentation, microsegmentation, virtual local area networks (VLANs), virtual routing

and forwarding (VRF), software-defined networking (SDN) and also emphasize œSecurity boundaries: secure zones, access control lists (ACLs), virtual private network (VPN) under Security Architecture. Why the other options are not the best choice:

A may improve cryptographic strength, but the configuration already shows SSH and HTTPS, so encrypted management access is already present. B is not the best answer because no unencrypted terminal service such as Telnet is shown in the configuration. D is generally useful operationally, but automatic patching and rebooting is not the main architectural weakness indicated by the config excerpt. The clearest risk visible in the router snippet is inadequate network scoping and boundary control, which points to segmentation as the best improvement.

Reference:

CompTIA SecurityX official exam objectives summary, Security Architecture domain. CompTIA SecurityX CAS-005 exam objectives PDF mirror containing the domain details for segmentation and security boundaries.

==========

QUESTION 332

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

Answer: D. Performing a supply chain analysis B

The best answer is B. Conducting an OSINT assessment. In the early phases of threat modeling, the analyst wants to understand the organizations 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. CompTIAs official SecurityX objectives include œGiven 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 organizations 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.

Reference:

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.

==========

QUESTION 333

An analyst needs to identify security event trends. The following is an excerpt from the SIEM: Time Alert Source Destination

20250407-UTC Successful login from uncommon auth method in 24 hours user1 AD-DC-01.corp

20250407-UTC User accessed sensitive resources user1 NFS-01/financial/share 20250407-UTC Potential password spraying from host 10.10.15.100 iga-server.corp 20250407-UTC Threshold exceeded user visiting high risk websites user2 freehacks.com 20250407-UTC Risk score exceeded for user user1 bar.ru

20250407-UTC NULL NULL NULL

Which of the following is the most practical way to identify trends?

A. Decreasing the timing window for detections related to user1

B. Incorporating audit log reduction

C. Correlating based on source field in batches of time

D. Disabling the noisy rules based on total alerts fired per day

Answer: C

The best answer is C. Correlating based on source field in batches of time. To identify trends in SIEM data, the analyst should group related events over a time window and correlate them around a common field. In this excerpt, user1 appears repeatedly across multiple alert types, including

unusual authentication, access to sensitive resources, and elevated risk score. That pattern is exactly the sort of repeated behavior that becomes visible when events are correlated by source over time. CompTIAs official SecurityX objectives in the Security Operations domain include œData analysis: indicators of malicious activity, trend analysis, statistics, and deduplication/correlation. That objective language directly supports this answer.

Why the other options are not best:

A narrows only one rule window and does not systematically identify trends across multiple event types. B may reduce volume, but reduction alone does not reveal trends. D is risky because noisy rules might still provide useful context, and disabling them based only on total daily alerts can hide meaningful multi-event patterns. The practical, operational approach is to correlate records by a shared field such as source/user across time batches so repeated suspicious behavior stands out.

Reference:

CompTIA SecurityX official exam objectives summary, Security Operations domain including trend analysis and correlation.

CompTIA SecurityX CAS-005 exam objectives PDF mirror with the same operational analysis themes.

QUESTION 334

John Doe's email account was compromised. The attacker's access to John Doe's account was removed and MFA was implemented. The attacker convinced Joe Roe in the accounting department to pay a fraudulent invoice through email exchanges. A security analyst is reviewing the headers from the initial email that Joe Roe received:

Received: from 221.15.11.103 (221.15.11.103.mta.com [221.15.11.103])

by with esmtps (TLS 1.2) Received-SPF: pass

Received: from 18.132.124.10 (18.132.124.10-internal.com [18.132.124.10]) by mx7sgwt-3S (Postfix) with ESMTPS id zRhQ22fmNnQCdys

DKIM-Signature: v=1; c=relaxed/relaxed; d=example.com; s=default; t=1672873468;

h=To: Message-ID: Date: Content-Type: Subject: From: From: To: Cc: Subject; To: jroe@example.com

Message-ID: _73/A4-32616-C36L8ZbYC4p

Date: Mon, 07 Apr 2025 +0000

Content-Type: multipart/alternative; boundary= MIME-Version: 1.0

Reply-To: jdoe@exampl.com

X- SpamProbability: 0.095349

Which of the following best explains how the attacker was able to get the invoice paid?

A. The attacker guessed John Doe's password.

B. The attacker registered a new domain.

C. The attacker's emails did not use domain keys for verification.

D. The email failed the sender policy framework check.

Answer: B

The best answer is B. The attacker registered a new domain. The key evidence is in the visible sender

fields: From: jdoe@exampl.com and Reply-To: jdoe@exampl.com. The legitimate company domain appears to be example.com, but the fraudulent email uses exampl.com, which is a lookalike domain missing the letter œe . That is a classic typosquatting/business email compromise pattern. The headers also show Received-SPF: pass, which means the message passed SPF for the domain it

actually came from, not that it was legitimate for the intended organization. The presence of a DKIMSignature also shows that lack of domain keys is not the issue. This is therefore best explained by an

attacker creating or registering a deceptive domain and sending authenticated email from it. CompTIA SecurityXs Security Operations domain includes activities around analyzing indicators, email artifacts, and attack patterns to identify malicious activity.

Why the other options are incorrect:

A is not the best explanation because the scenario says John Does account had been compromised earlier, but the specific headers here point to a spoof-like lookalike domain attack, not necessarily

direct reuse of Johns real mailbox. C is incorrect because the headers explicitly show a DKIMSignature, so domain keys were used. D is incorrect because the headers show Received-SPF: pass,

not fail. The payment succeeded because the attacker used a deceptive domain that looked close enough to the legitimate one to fool the recipient during the invoice exchange.

Reference:

CompTIA SecurityX official exam objectives summary, especially Security Operations skills around analyzing malicious activity and indicators.

CompTIA SecurityX CAS-005 exam objectives PDF mirror.

==========

QUESTION 335

An analyst must remediate vulnerabilities in IoT devices within 24 hours. These vulnerabilities: Have CVSS scores of less than 7.0

Have updates available

Will not significantly impact production systems if remediation is unsuccessful Which of the following practices is best for the analyst to use to resolve the issue?

B. Vulnerability prioritization

C. Forced restart of the device

Answer: D. SOAR playbook creation A

The best answer is

A. Automated patching. The scenario already states that updates are available,

the vulnerabilities must be remediated within 24 hours, and the risk of unsuccessful remediation is low because production impact would not be significant. That makes direct, rapid deployment of fixes the most appropriate practice. CompTIAs SecurityX objectives include operational response and automation themes, and the official exam summary explicitly references automation capabilities in multiple areas. In this scenario, automation is not just helpful; it is the most practical way to meet the time requirement consistently across IoT devices.

Why the other options are incorrect:

B. Vulnerability prioritization is something you do before deciding what to remediate first, but the question already gives the prioritization context and asks how to resolve the issue. C. Forced restart does not remediate the vulnerabilities. D. SOAR playbook creation might support a broader workflow in the future, but creating a playbook is slower and less direct than simply using automated patching when patches already exist and risk is acceptable. Under the stated conditions, automated patching

is the best-fit operational response.

Reference:

CompTIA SecurityX official exam objectives summary. CompTIA SecurityX CAS-005 exam objectives PDF mirror.

==========

QUESTION 336

A security officer performs due diligence activities before implementing a third-party solution into the enterprise environment. The security officer needs evidence from the third party that a data subject access request handling process is in place. Which of the following is the security officer most likely seeking to maintain compliance?

A. Information security standards

B. E-discovery requirements

C. Privacy regulations

D. Certification requirements

Answer: E. Reporting frameworks C

The best answer is C. Privacy regulations. A data subject access request process exists to support an individuals right to access their personal data. Regulators and official privacy guidance define this as a core privacy right. The UK ICO explains that the œright of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data , and Article 15 GDPR establishes the same right in law. Because the security officer is asking a third party to prove it can handle these requests, the officer is clearly validating compliance with privacy law and related data protection obligations.

This also aligns with CompTIA SecurityXs GRC focus on compliance requirements, program documentation, and data governance. A third party that processes personal data for the enterprise must be able to respond appropriately to access requests from data subjects, so confirming that process is a due diligence activity tied to regulatory privacy compliance rather than e-discovery, certification, or generic reporting frameworks.

Why the other options are incorrect:

A . Information security standards may require good practices, but DSAR handling is specifically about privacy rights. B. E-discovery requirements relate to legal discovery and litigation processes, not an individuals privacy access rights. D. Certification requirements and E. Reporting frameworks are not the primary reason an organization must support subject access requests. The clearest and most accurate answer is privacy regulations.

Reference:

ICO guidance on subject access requests and the right of access. UK/EU GDPR Article 15, right of access by the data subject.

CompTIA SecurityX official exam objectives summary, GRC domain. CompTIA SecurityX CAS-005 exam objectives PDF mirror.

QUESTION 337

An engineer is designing a solution that addresses the following requirements: The security controls must be redundant.

The security operations cannot be entirely disrupted by a supply chain attack. The systems must be resilient and better prepared for zero-day vulnerabilities. Which of the following is the best way to meet these requirements?

A. Leveraging a managed service provider to support operations

B. Acquiring security solutions from a single vendor for seamless integration

C. Migrating current security solutions to the cloud

Answer: D. Deploying heterogeneous security solutions to offer a layered approach D

The best answer is D. Deploying heterogeneous security solutions to offer a layered approach. The

Why the other options are not best:

A may add support capacity, but it does not inherently provide redundant, diverse technical controls.

B is the opposite of the requirement because a single-vendor stack increases supply-chain concentration risk. C may change hosting model, but cloud migration alone does not guarantee redundancy against supply-chain compromise or zero-day resilience. A layered heterogeneous design is the strongest match to all three requirements.

Reference:

CompTIA SecurityX official exam objectives summary, especially Security Architecture themes of layered controls and resilience.

==========

QUESTION 338

An application security engineer is examining the IAM configuration for a workload. The following is a sample of the decoded payload and header:

"alg": "None"

"typ": "JWT"

"user": "98765"

"iat": 1680000000

"exp": 1680003600

"sub": "svc account" "refresh": true "token_id": "abc123"

Which of the following is the most concerning risk?

A. Lateral movement

B. Privilege escalation

C. Credential stuffing

Answer: D. RCE from deserialization B

The best answer is B. Privilege escalation. The most critical issue is the JWT header value "alg": "None", which indicates an unsigned token. If a workload accepts such a token, an attacker may be

Why the other options are not best:

A . Lateral movement could be a downstream result, but the immediate and primary risk in the token itself is unauthorized privilege gain. C. Credential stuffing involves reuse of stolen usernames and passwords, which is unrelated to this JWT issue. D. RCE from deserialization is a different application vulnerability class and is not the main concern shown by the JWT header and claims. The most direct risk here is privilege escalation via forged or altered tokens.

Reference:

CompTIA SecurityX official exam objectives summary, including IAM-related secure control implementation.

==========

QUESTION 339

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

Answer: D. Using compliance baselines in the MDM to ensure all endpoints receive the required agents B

The best answer is B. Implementing Conditional Access with device certifications and compliance requirements. The CISOs 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. CompTIAs 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

Reference:

CompTIA SecurityX official exam objectives summary, especially IAM and enterprise access-control enforcement themes.

==========

QUESTION 340

A security analyst receives the following SIEM alert for review:

Time | Event

03/075 UTC 13:54:06 | MACHINE: hr_talent_01.corp.local "cd" SUCCESS 03/075 UTC 13:54:07 | MACHINE: hr_talent_01.corp.local "cd ../../" SUCCESS

03/075 UTC 13:54:08 | MACHINE: hr_talent_01.corp.local "sudo cat /etc/shadow" SUCCESS Which of the following best describes the incident that occurred on the device?

A. A file injection attack occurred on the device.

B. An attacker viewed password hashes on the device.

C. A sensitive file was exfiltrated from the device.

D. A directory traversal attack occurred on the device.

Answer: B

The best answer is B. An attacker viewed password hashes on the device. The decisive event is sudo cat /etc/shadow SUCCESS. On Linux systems, /etc/shadow stores password hashes and related account password data. The log therefore indicates successful privileged access to that file and successful viewing of its contents. CompTIAs SecurityX Security Operations domain includes analysis of indicators of malicious activity and investigation of suspicious system behavior; this command sequence is consistent with credential-access activity.

Why the other options are not best:

A is incorrect because there is no evidence of file injection. C is not supported because the logs show file access, not confirmed data transfer or exfiltration. D is tempting because of cd ../../, but that is only navigation. The key security-relevant action is the successful reading of /etc/shadow, which means password hashes were viewed.

Reference:

CompTIA SecurityX official exam objectives summary, Security Operations domain.

==========

QUESTION 341

A water power generation plant fails a security inspection. The controllers are distributed across a river that is 0.5mi (0.8km) wide. The controllers are connected via HTTP to the shoreside master

A. Monitoring control traffic for command sequences with out-of-range or unexpected values

B. Disconnecting cellular radios in favor of shielded Cat 5e cables to each of the controllers

C. Reviewing the ladder logic on the controllers to determine whether unauthorized changes have been introduced

Answer: D. Deploying a dedicated base station and reducing the footprint with highly directional antennas D

The best answer is D. Deploying a dedicated base station and reducing the footprint with highly directional antennas. The biggest risk in the scenario is that unencrypted control traffic is traversing the internet over a cellular network. Since encryption is not feasible, the best compensating control is to reduce exposure by making the wireless path more private, more local, and less accessible to unintended parties. A dedicated base station with directional antennas narrows the RF footprint and reduces interception and unauthorized access opportunities compared with broad internet-based

cellular exposure. CompTIAs SecurityX objectives emphasize Security Architecture, including secure boundaries, compensating controls, and resilient design choices when ideal controls cannot be used.

Why the other options are not best:

A is helpful as a detective control, but it does not reduce the core exposure of unencrypted communications over public infrastructure. B is impractical and technically weak here; standard Cat 5e is not the right medium for a 0.5-mile river crossing. C may detect post-compromise changes, but it does not reduce the likelihood of network compromise in the first place. Because encryption cannot be used, the best risk-reduction strategy is to minimize signal exposure and dependence on public internet-connected cellular paths.

Reference:

CompTIA SecurityX official exam objectives summary, especially Security Architecture and compensating-control themes.

QUESTION 342

An organization with a remote workforce has a new client with the following requirements: Consultants need to travel to the client site.

The company has proprietary information on its hard drives. The company prohibits BYOD.

Which of the following would be the most beneficial for the organization to implement?

A. Virtual hardware

B. Measured boot

Answer: D. Host-based encryption D

The best answer is D. Host-based encryption. The strongest clue is that the company has proprietary information on its hard drives and consultants must travel with company-managed devices because BYOD is prohibited. That makes protection of data at rest on the endpoint the primary concern. Hostbased encryption protects the contents of the drive if a laptop is lost, stolen, or physically accessed

during travel. CompTIAs SecurityX certification emphasizes building secure solutions across complex environments and supporting resilient enterprise protection, which includes securing endpoints and sensitive data stored on them.

Why the other options are not best:

A . Virtual hardware does not directly protect the data on the hard drive if the device is lost or stolen.

B. Measured boot helps validate platform integrity at startup, but it does not primarily protect confidential data at rest. C. Secure enclave can protect certain secrets and key material, but it is narrower than full host-based encryption for an entire laptop drive. Because the requirement is specifically about proprietary data on traveling endpoints, full device or host-based encryption is the most beneficial control.

Reference:

CompTIA SecurityX official certification page describing secure solution design across complex environments.

==========

QUESTION 343

An organization's vulnerability management team is reviewing the following output from a scan of a production server:

Finding ID | Summary

Weak cryptographic library | The device allows the use of weak cryptographic libraries.

End-of-life, third-party library | The running service includes an end-of-life, third-party library. Remote service detected | The device is running FTP on TCP port 21.

End-of-life operating system | The operating system has reached end-of-life status. Database detected | This device includes an installed database.

Which of the following should the team do first?

A. Deploy a bastion host in front of the devices.

B. Close the ports to the database service.

C. Upgrade to a manufacturer-supported operating system.

D. Disable the running FTP service.

Answer: C

The best answer is C. Upgrade to a manufacturer-supported operating system. The end-of-life operating system is the highest-priority foundational issue because it affects the overall security posture of the host. An unsupported OS no longer receives vendor security updates, which increases exposure across the entire system, including services and libraries running on it. From a SecurityX perspective, vulnerability management and asset lifecycle issues are part of security operations and enterprise resilience. Resolving the unsupported platform first addresses the broadest root problem. CompTIAs SecurityX exam coverage includes security operations, vulnerability management activities, and proper hardware/software asset management as core skills.

Why the other options are weaker as the first step:

A adds a compensating control but leaves the unsupported server in place. B may be appropriate later, but the prompt does not indicate the database service is the primary exposed weakness. D disabling FTP would remove an insecure service and is a good hardening step, but it still leaves the system on an unsupported operating system with broader unpatched risk. The first action should address the most systemic weakness, which is the end-of-life OS.

Reference:

CompTIA SecurityX official certification page.

CompTIA blog summary of current security operations topics including vulnerability management and asset management.

==========

QUESTION 344

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

Initial report:

Device | Type | EDR status | Infection Status

LN002 | Linux SE | Enabled (unmanaged) | Unknown OWIN23 | Windows 7 | Enabled | Clean

OWIN29 | Windows 10 | Enabled (bypass) | Clean MAC005 | Mac OS | Enabled | Clean

After five days:

Device | Type | EDR status | Infection Status

LN002 | Linux SE | Enabled (unmanaged) | Unknown OWIN23 | Windows 7 | Enabled | Clean

OWIN29 | Windows 10 | Enabled (bypass) | Infected MAC005 | Mac OS | Disabled | Clean

Which of the following most likely enabled the infection?

A. OWIN23 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. OWIN29's EDR has an unknown vulnerability that was exploited by the attacker.

Answer: C

The best answer is C. OWIN29's EDR has an unknown vulnerability that was exploited by the attacker. The decisive clue is that OWIN29 had EDR status: Enabled (bypass) in both reports and changed from Clean to Infected after five days. That strongly indicates the endpoint protection on that host was

being bypassed, allowing compromise despite the agent being present. In SecurityX terms, this fits the theme of resilience against advanced threats and the possibility that a defensive tool can be circumvented or affected by a zero-day or other unknown weakness. CompTIAs SecurityX certification emphasizes designing and operating secure solutions that remain resilient in the face of modern threats.

Why the other options are less likely:

A is not supported because OWIN23 remained Clean. B is speculative; LN002 stayed Unknown, but there is no evidence it propagated malware to OWIN29. D is also unsupported because MAC005 was Clean even after its EDR became disabled. The only host with a direct clue pointing to failed protection and subsequent infection is OWIN29, making the EDR bypass or exploitation on that host the most likely cause.

Reference:

CompTIA SecurityX official certification page.

QUESTION 345

4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 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 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 00 04 00 00 00 00 00 00 00 00 60 01 00 00 02 00 00 00

00 00 00 03 00 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 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

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 hexencoded 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.

Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 5: "Malware Analysis," Section

5.3: "Static and Dynamic Analysis Techniques."

QUESTION NO: 16

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. Performattack surface reduction.

C. Disable third-party integrations.

D. Limit access to the systems.

ANSWER: B

Explanation:

Performattack surface reduction is correct because the stated goal is to minimize the number of exposed services and reduce the opportunities an adversary has to interact with, probe, or exploit systems. Attack surface reduction is the broad security engineering practice of identifying exposed components, removing unnecessary functionality, closing unused ports, disabling unneeded services, and hardening externally reachable interfaces. As a first step, it gives the architect a structured way to inventory what is exposed, determine what is required for business operations, and eliminate or restrict everything else. This aligns closely with the principle of least functionality described in NIST SP 800-53, which requires systems to provide only essential capabilities and to prohibit or restrict unnecessary functions, ports, protocols, and services. It is also consistent with Microsoft’s attack surface reduction guidance, which frames ASR as reducing the places where an organization is vulnerable to attack. See NIST SP 800-53 Revision 5 and Microsoft Defender attack surface reduction overview.

QUESTION NO: 17

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

A. Differential power analysis

B. Differential fault analysis

C. Differential temperature analysis

D. Differential timing analysis

ANSWER: B

Explanation:

Differential fault analysis is correct because the attack described relies on intentionally forcing the smart card into an abnormal operating condition so that cryptographic processing produces faulty or exploitable results. In smart card and embedded cryptographic hardware testing, environmental stress such as abnormal temperature, voltage glitches, clock manipulation, or other induced disturbances can cause computation errors during cryptographic operations. By comparing normal outputs with faulty outputs, or by analyzing how the device behaves under the induced fault, an attacker may be able to infer internal state information and ultimately recover secret key material. This is the defining idea behind fault-based side-channel cryptanalysis: the attacker actively perturbs the device rather than merely observing passive characteristics. High temperature is therefore a plausible fault-injection method against a physical cryptographic token such as a smart card. For additional background, see OWASP's discussion of fault injection in hardware attacks at OWASP Fault Injection and the original differential fault analysis concept described by Biham and Shamir at IACR Cryptology ePrint/cryptographic paper index.

QUESTION NO: 18

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

A. Threat hunting

B. A system penetration test

C. Log analysis within the SIEM tool

D. The Cyber Kill Chain

ANSWER: A

Explanation:

Threat hunting is correct because it is the proactive SOC activity used to take new threat intelligence—such as details about an active campaign, exploited vulnerability, indicators of compromise, malware behavior, or adversary tactics—and search the organization's environment for evidence of exposure, attempted exploitation, or compromise. In this scenario, the company is not simply asking for a general security assessment; it has campaign-specific intelligence and wants to determine whether that threat is relevant to its own systems. A threat hunt can translate the intelligence into hypotheses and queries, then examine endpoint telemetry, network traffic, asset data, vulnerability context, and SIEM/EDR events to identify whether affected assets or related attacker behaviors are present. This aligns with how modern SOCs operationalize threat intelligence: they use it to guide targeted hunts and rapidly assess organizational impact. MITRE describes cyber threat intelligence as supporting detection and response by informing searches for adversary behavior, and CISA also emphasizes using threat information to help organizations identify and reduce exposure to active threats. References: MITRE ATT&CK and CISA Cyber Threats and Advisories.

QUESTION NO: 19

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: B

Explanation:

Create an acceptable use policy is the best first step because the problem described is primarily user behavior, not confirmed data leakage. The DLP tool is detecting employees sending messages from corporate accounts to their own personal accounts, but the messages do not contain company data. Before applying broad technical restrictions, the organization should establish and communicate clear rules for appropriate corporate email use, including whether employees may send messages to personal accounts, under what circumstances, and what types of data or activity are prohibited. An acceptable use policy gives the security team a governance basis for user guidance, monitoring, exception handling, and future enforcement if the behavior continues. This aligns with common security governance practice: define policy and expected behavior first, then support it with technical controls and training. NIST describes “rules of behavior” as documented expectations for system users, which is directly related to acceptable use governance: NIST SP 800-53 PL-4. CompTIA SecurityX also emphasizes governance, risk, and compliance concepts as part of enterprise security operations: CompTIA SecurityX.

QUESTION NO: 20

A development team created a mobile application that contacts a company’s back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.

Which of the following would BEST safeguard the APIs? (Choose two.)

A. Bot protection

B. OAuth 2.0

C. Input validation

D. Autoscaling endpoints

E. Rate limiting

F. CSRF protection

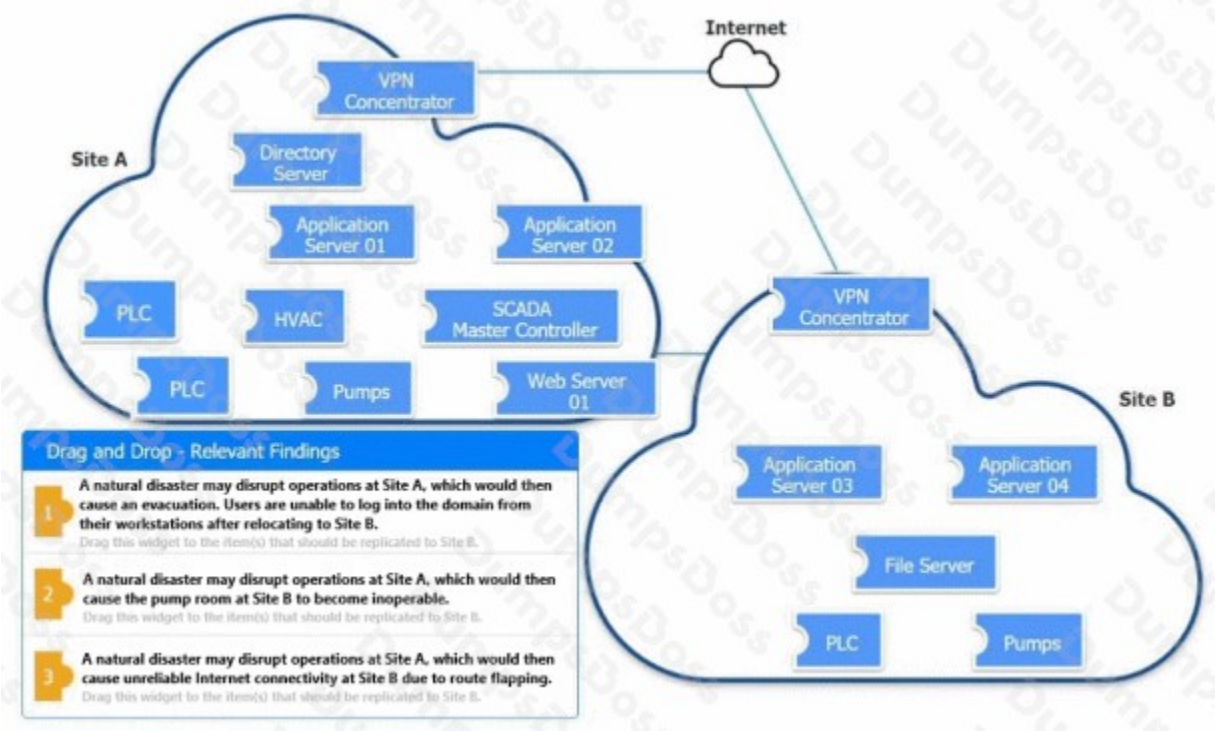
ANSWER: A E

Explanation:

Bot protection and rate limiting are the best safeguards for APIs experiencing high processor utilization from scraping activity. Bot protection is designed to distinguish legitimate application or user traffic from automated scraping, credential stuffing, and other unwanted automated behavior. In an API context, this can include bot scoring, device or client fingerprinting, JavaScript or SDK-based challenges where appropriate, behavioral analytics, and blocking known malicious automation patterns before those requests consume back-end resources. Rate limiting complements this by enforcing request thresholds per client, IP address, token, API key, user, or route. This directly reduces excessive request volume and helps keep API CPU utilization within acceptable limits while still allowing normal mobile application usage. Together, these

controls both prevent abusive automated access and contain the operational impact when scraping attempts occur. This aligns with common API security guidance that recommends throttling and automated abuse protections for protecting API availability and preventing resource exhaustion. Relevant guidance is available from OWASP API Security Top 10: Unrestricted Resource Consumption and OWASP REST Security Cheat Sheet.

QUESTION NO: 21 - (DRAG DROP)



An organization is planning for disaster recovery and continuity of operations.

INSTRUCTIONS

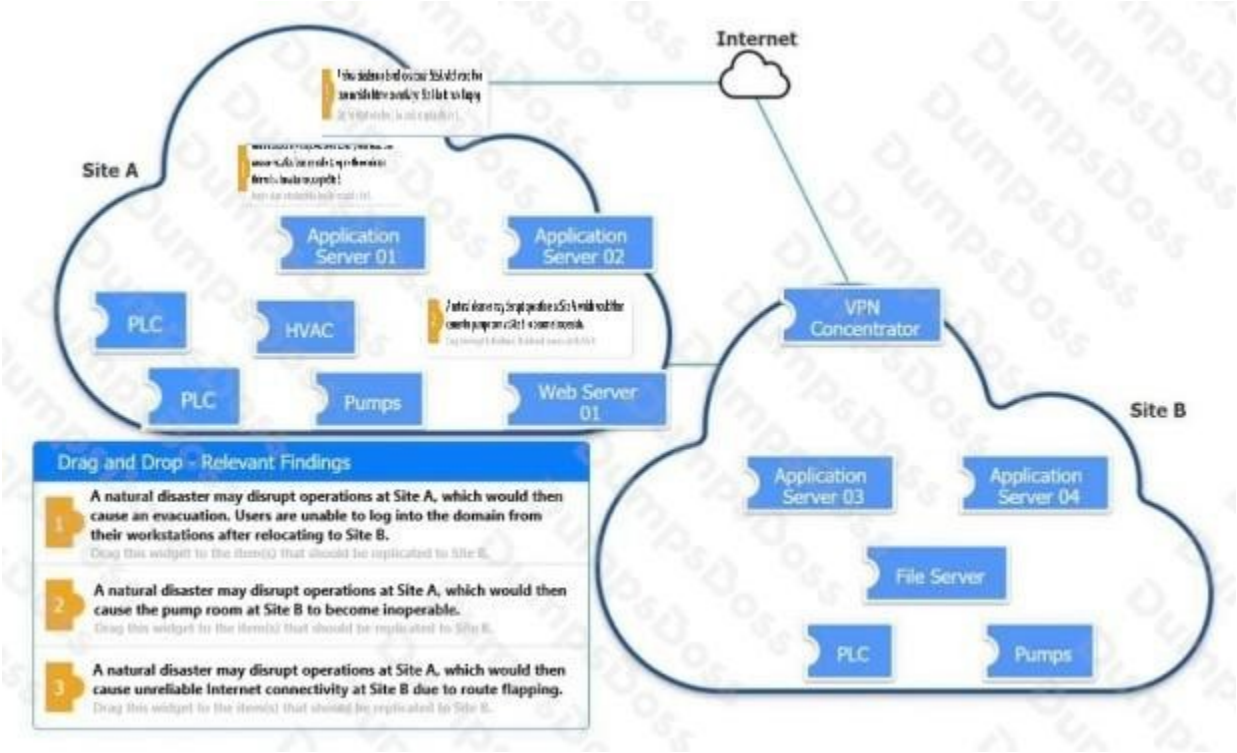
Review the following scenarios and instructions. Match each relevant finding to the affected host.

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 simul-ation, please click the Reset All button.

ANSWER:



Explanation:

The correct continuity design focuses on replicating the services that Site B would need if Site A were unavailable. A directory service must be available at the recovery location because relocated users still need to authenticate, receive domain policy, and access domain resources. In practice, that means the Site A Directory Server function should be replicated or otherwise made available at Site B so authentication does not depend on the failed site. This aligns with contingency planning guidance that identifies critical systems and recovery dependencies before a disruption, such as the approach described in NIST SP 800-34 Revision 1.

The SCADA Master Controller is also a critical dependency because it coordinates industrial control operations. If Site B pump operations depend on the master controller located at Site A, then losing Site A would affect the pump room even though the pump equipment is physically at Site B. Replicating that controller capability supports operational resilience for industrial control systems, which is consistent with the availability and continuity concerns discussed in NIST SP 800-82 Revision 3.

For the route-flapping issue, the relevant host is the VPN Concentrator because it participates in site connectivity and routing. The corrective action should be route-flap damping or route dampening on the VPN/routing device, which suppresses unstable routes so repeated up/down route advertisements do not continuously disrupt connectivity. Route flap damping is a standard mechanism documented in RFC 2439. Together, these selections preserve authentication, industrial control, and stable network failover during a Site A disaster.

QUESTION NO: 22

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.

B. Implement an XML gateway and monitor for policy violations.

C. Monitor dependency management tools and report on susceptible third-party libraries.

D. Install an IDS on the development subnet and passively monitor for vulnerable services.

E. Model user behavior and monitor for deviations from normal.

F. Continuously monitor code commits to repositories and generate summary logs.

ANSWER: E F

Explanation:

Continuously monitor code commits to repositories and generate summary logs is correct because unauthorized insertions into a development environment are most directly detected through visibility into source-control activity. Commit metadata, branch activity, pull requests, author identity, timestamps, and change summaries give the SOC the audit trail needed to identify unexpected code additions, suspicious commit patterns, and potential software supply chain compromise. Modern secure development guidance emphasizes protecting and monitoring source code repositories as part of software supply chain security, as described in CISA secure software development resources.

Model user behavior and monitor for deviations from normal is also correct because the second scenario involves authorized insiders performing unauthorized configuration changes. Since the user may have valid credentials, detection depends less on simple authentication failure events and more on behavioral analytics: unusual access times, abnormal configuration targets, atypical privilege use, unexpected change volume, or activity inconsistent with the user's role. These feeds support insider-threat and entity behavior analytics in the SOC. NIST highlights the importance of logging, monitoring, and analyzing events to detect anomalous or unauthorized activity in systems and development processes; see NIST SP 800-53 Rev. 5.

QUESTION NO: 23

Third partiesnotified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

A. Using IaC to include the newest dependencies

B. Creating a bug bounty program

C. Implementing a continuous security assessment program

D. Integrating a SASI tool as part of the pipeline

E. Integrating a software composition analysis (SCA) tool as part of the pipeline

ANSWER: E

Explanation:

Integrating a software composition analysis (SCA) tool as part of the pipeline is correct because the issue is specifically tied to previously disclosed vulnerabilities in third-party libraries. SCA tools inventory open-source and commercial dependencies, compare them against vulnerability databases such as CVE/NVD and vendor advisories, and identify affected package versions during development and build processes. Placing SCA in the CI/CD pipeline helps teams detect vulnerable libraries before release, fail builds when risk thresholds are exceeded, and guide developers toward patched versions or safer alternatives. This directly addresses the root cause: vulnerable external components embedded in the application supply chain. It also supports modern secure software development practices by continuously monitoring dependency risk as new vulnerabilities are disclosed after code has already been written. OWASP describes dependency and component tracking as a key activity for identifying known vulnerable components, and tools such as OWASP Dependency-Check and Dependency-Track are common examples of this control. See OWASP Dependency-Check and OWASP Dependency-Track.

QUESTION NO: 24

A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process '

A. Request a weekly report with all new assets deployed and decommissioned

B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.

C. Implement a shadow IT detection process to avoid rogue devices on the network

D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

ANSWER: D

Explanation:

Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool is correct because the core issue is asset volatility. When devices and IP addresses are frequently added, removed, or reassigned, vulnerability reports become unreliable unless the scanner continuously refreshes its view of the environment. Discovery scanning helps the organization identify active hosts, services, and network ranges before or alongside vulnerability assessment, keeping the asset inventory aligned with what is actually present on the network. That makes subsequent vulnerability findings more complete, current, and repeatable.

In a mature vulnerability management process, asset discovery is not a one-time setup task; it is a continuous or regularly scheduled activity that supports accurate scoping, prioritization, and remediation tracking. This aligns with vulnerability management best practices that emphasize maintaining awareness of assets and continuously identifying exposures across the enterprise. NIST describes vulnerability management as an ongoing process involving identifying, assessing, and remediating vulnerabilities, while CISA's continuous vulnerability management guidance also highlights ongoing discovery and assessment as foundational activities. See NIST SP 800-40 Rev. 4 and CISA Continuous Vulnerability Management.

QUESTION NO: 25

A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

A. SD-WAN

B. PAM

C. Remote access VPN

D. MFA

E. Network segmentation

F. BGP

G. NAC

ANSWER: B C E

Explanation:

PAM, Remote access VPN, and Network segmentation are the best remediation choices because they directly address the consultant's three major findings. PAM provides privileged access governance through least privilege, approval workflows, credential vaulting, session monitoring, and just-in-time administrative access, which is the right control when privileged access is not limited. Remote access VPN helps eliminate direct, open RDP exposure by requiring users to connect through an authenticated, controlled remote access path before reaching internal systems that contain personal health information. Network segmentation addresses the flat network by separating sensitive systems, such as PHI servers, from general user networks and by enforcing traffic controls between zones. Together, these controls reduce ransomware blast radius, limit

lateral movement, and make administrative access more auditable and defensible. This aligns with ransomware hardening guidance that recommends restricting remote services such as RDP and applying least-privilege access controls, as described by CISA's Ransomware Guide. It also aligns with NIST access control guidance for least privilege and controlled system access in NIST SP 800-53 Rev. 5.

QUESTION NO: 26

A company needs to quickly assess whether software deployed across the company ' s global corporate network contains specific software libraries. Which of the following best enables the company ' s SOC to respond quickly when such an assessment is required?

A. Maintaining SAST/DAST reports on a server with access restricted to SOC staff

B. Contractually requiring all software vendors to attest to third-party risk mitigations

C. Requiring all suppliers and internal developers to implement a thorough SBoM

D. Implementing a GRC tool to maintain a list of all software vendors and internal developers

ANSWER: C

Explanation:

Requiring all suppliers and internal developers to implement a thorough SBoM is correct because a Software Bill of Materials provides a structured inventory of the components, dependencies, and libraries included in software. For a SOC, this is especially valuable during time-sensitive events such as disclosure of a widely used vulnerable library. Instead of manually asking application teams or vendors whether a package is present, analysts can query SBOM data to identify affected products and prioritize remediation quickly across the enterprise.

An SBOM supports software supply chain visibility by documenting direct and transitive components, versions, suppliers, and related metadata in machine-readable formats such as SPDX or CycloneDX. This enables faster vulnerability impact analysis, better asset correlation, and more consistent response when new CVEs affect common open-source or third-party libraries. U.S. government guidance also emphasizes SBOMs as a key mechanism for improving transparency and managing software supply chain risk. See CISA Software Bill of Materials and NTIA Software Bill of Materials.

QUESTION NO: 27

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of the impact. Which of the following should the organization perform next?

A. Assess the residual risk.

B. Update the organization's threat model.

C. Move to the next risk in the register.

D. Recalculate the magnitude of the impact.

ANSWER: A

Explanation:

Assess the residual risk is correct because mitigation does not eliminate the risk; it changes the organization's remaining exposure. After controls or compensating measures are applied, security teams should determine the residual risk by reassessing the likelihood and impact in light of the new control state. This confirms whether the remaining risk is within the organization's risk appetite or tolerance and whether additional treatment, acceptance, transfer, or escalation is required. In practical risk management, this step also provides governance evidence that mitigation was effective and that leadership can make an informed decision about the remaining exposure. NIST describes risk assessment as including determination of likelihood, impact, and risk, and risk response as selecting and implementing ways to address identified risk; after response

actions, the remaining risk must be understood and managed. See NIST SP 800-30 Rev. 1 and NIST SP 800-37 Rev. 2 for related risk assessment and risk management guidance.

QUESTION NO: 28

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

Explanation:

Using the existing MDM solution to integrate with directory services for authentication and enrollment is correct because MDM is the standard scalable control plane for configuring thousands of mobile devices. It can push WLAN/NAC profiles, bind enrollment to corporate identity, and coordinate certificate deployment without requiring administrators to touch each device manually. This aligns well with enterprise PKI operations because device identity, user identity, and policy assignment can be centrally managed and audited.

Configuring SCEP on the CA with an OTP for bulk device enrollment is also correct because Simple Certificate Enrollment Protocol is commonly used by MDM platforms to automate certificate issuance to managed endpoints. The one-time password or challenge mechanism helps authorize enrollment while still supporting high-volume deployment, which is important when moving a large mobile fleet to certificate-based WLAN authentication such as EAP-TLS. Microsoft documents this pattern for Intune-managed devices using SCEP certificate profiles: Configure infrastructure to support SCEP with Intune. The protocol itself is also described by the IETF here: RFC 8894 - Simple Certificate Enrollment Protocol.

QUESTION NO: 29

An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

A. Regression testing

B. SAST

C. Third-party dependency management

D. IDE SAST

E. Fuzz testing

F. IAST

ANSWER: B E

Explanation:

SAST is correct because static application security testing can be used to examine an application without executing it, and many static analysis tools can assess compiled artifacts such as binaries or bytecode when source code is unavailable. In a software assurance program, this supports pre-production vetting by identifying insecure functions, known vulnerability patterns, hardcoded secrets, unsafe calls, and other weaknesses through static inspection. Fuzz testing is also correct because it does not require source code; it exercises the compiled application by sending malformed, unexpected, or random inputs to discover crashes, memory corruption, input-validation flaws, and other runtime defects. Together, these approaches are well suited for binary-only applications because they provide complementary coverage: SAST inspects the artifact statically, while fuzz testing observes how the executable behaves under abnormal input conditions. OWASP describes static analysis tools as capable of analyzing source code or compiled code, and OWASP also identifies fuzzing as a technique for submitting invalid or random data to uncover implementation weaknesses. References: OWASP Source Code Analysis Tools and OWASP Fuzzing.

QUESTION NO: 30

An organization ' s vulnerability management team is reviewing the following output from a scan of a production server:

Finding ID | Summary

Weak cryptographic library | The device allows the use of weak cryptographic libraries.

End-of-life, third-party library | The running service includes an end-of-life, third-party library.

Remote service detected | The device is running FTP on TCP port 21.

End-of-life operating system | The operating system has reached end-of-life status.

Database detected | This device includes an installed database.

Which of the following should the team do first?

A. Deploy a bastion host in front of the devices.

B. Close the ports to the database service.

C. Upgrade to a manufacturer-supported operating system.

D. Disable the running FTP service.

ANSWER: C

Explanation:

Upgrade to a manufacturer-supported operating system. is the correct first action because an end-of-life operating system represents a foundational vulnerability-management problem. Once an operating system is no longer supported by the manufacturer, it generally no longer receives routine security patches, defect fixes, or vendor-backed remediation guidance. That means newly discovered vulnerabilities in the platform may remain permanently unpatched, increasing risk for every service, library, and application running on the server. In a production environment, the vulnerability management team should prioritize remediation that restores the asset to a supportable, patchable state so future security updates can be applied through normal lifecycle and change-management processes.

This aligns with accepted vulnerability and asset lifecycle practices: unsupported software should be upgraded, replaced, or removed because it cannot be maintained securely over time. NIST's guidance on vulnerability management emphasizes identifying, prioritizing, and remediating weaknesses across systems, including maintaining software so security updates can be applied. See NIST SP 800-40 Rev. 4. CISA also highlights the operational risk of unsupported products and encourages organizations to plan migrations before end-of-support dates; see CISA guidance on end-of-support software.

QUESTION NO: 31

city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:

+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.

+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.

+ Ransomware threats and zero-day vulnerabilities must be quickly identified.

Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection

B. Log aggregator

C. Zero trust network access

D. PAM

E. Cloud sandbox

F. SIEM

G. NGFW

ANSWER: B D F

Explanation:

Log aggregator, PAM, and SIEM are the best fit for the stated grant requirements because they collectively address long-term evidence retention, privileged access governance, and security monitoring. A log aggregator provides centralized collection and storage of logs from critical systems, which supports the 365-day retention requirement and gives analysts a dependable source of historical telemetry for investigations and threat hunting. NIST's guidance on log management emphasizes centralized collection, analysis, storage, and retention as core log management functions: NIST SP 800-92. PAM directly supports tight control and tracking of privileged users by enforcing least privilege, credential vaulting, session monitoring, approval workflows, and auditing for administrative activity. SIEM complements the logging layer by correlating events, applying analytics and threat intelligence, and generating alerts that help security teams quickly identify ransomware behavior and suspicious activity associated with emerging or zero-day exploitation. Microsoft's SIEM overview describes this type of centralized security analytics, detection, and incident response capability: Microsoft Sentinel documentation.

QUESTION NO: 32

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

1. International users reported latency when images on the web page were initially loading.

2. During times of report processing, users reported issues with inventory when attempting to place orders.

3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.

C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.

D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

ANSWER: A

Explanation:

Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance is the best design because it directly addresses all three observed availability and performance problems with appropriate cloud-native patterns. A distributed content delivery network caches images and other static assets at edge locations closer to international users, reducing initial page-load latency and offloading traffic from the origin service. Using a read replica for reporting separates read-heavy analytics workloads from the transactional inventory and ordering database, helping ensure that report generation does not contend with live order processing. Performance-based auto-scaling for API servers is also important because a fixed number of servers does not guarantee adequate capacity during seasonal peaks; scaling policies can add or remove compute resources dynamically based on metrics such as CPU utilization, request count, or latency. These controls align with common cloud architecture best practices for elasticity, workload isolation, and global content delivery. See Microsoft Azure architecture guidance on autoscaling and AWS CloudFront documentation for supporting design principles.

QUESTION NO: 33

The device event logs sourced from MDM software are as follows:

Device | Date/Time | Location | Event | Description

ANDROID_102 | 01JAN21 0255 | 38.9072N, 77.0369W | PUSH | APPLICATION 1220 INSTALL QUEUED

ANDROID_102 | 01JAN21 0301 | 38.9072N, 77.0369W | INVENTORY | APPLICATION 1220 ADDED

ANDROID_1022 | 01JAN21 0701 | 39.0067N, 77.4291W | CHECK-IN | NORMAL

ANDROID_1022 | 01JAN21 0701 | 25.2854N, 51.5310E | CHECK-IN | NORMAL

ANDROID_1022 | 01JAN21 0900 | 39.0067N, 77.4291W | CHECK-IN | NORMAL

ANDROID_1022 | 01JAN21 1030 | 39.0067N, 77.4291W | STATUS | LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would best address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220

B. Resource leak; recover the device for analysis and clean up the local storage

C. Impossible travel; disable the device ' s account and access while investigating

D. Falsified status reporting; remotely wipe the device

ANSWER: C

Explanation:

Impossible travel; disable the device ' s account and access while investigating is the best answer because the MDM check-ins show the same device identifier reporting from two geographically distant locations at the exact same time. Coordinates near Virginia in the United States and Doha, Qatar cannot realistically be associated with one physical device at the same timestamp, so the event pattern is a high-confidence indicator of compromise, device cloning, token theft, or fraudulent enrollment/check-in activity. The safest response is to immediately contain the potential compromise by disabling the device’s account and access, preventing continued use of enterprise resources while security teams validate ownership, review authentication records, inspect enrollment status, and determine whether credentials or device certificates have been misused. This aligns with mobile device management best practices: when a managed device or its identity is suspected to be compromised, administrators should restrict access and investigate before restoring trust. NIST guidance for mobile device security emphasizes centralized management, access control, and response capabilities for compromised mobile endpoints; see NIST SP 800-124 Rev. 2. CISA also highlights protecting mobile devices and accounts from unauthorized access in its Mobile Device Cybersecurity Best Practices.

QUESTION NO: 34

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 arc the most appropriate? (Select two).

A. Federation

Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.

B. Micro segmentation

Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.

C. CASB

D. PAM

PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.

E. SD-WAN

SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.

F. SASE

ANSWER: C F

Explanation:

CASB and SASE are the most appropriate solutions because together they address cloud access control, traffic enforcement, and identity-aware security. CASB provides a control point between users and cloud services, giving organizations visibility into cloud application use, policy enforcement, threat protection, and data protection for sanctioned and unsanctioned cloud resources. A CASB commonly integrates with enterprise identity providers so access decisions can be based on user identity, group membership, device posture, location, and risk context. Microsoft describes CASB capabilities as including visibility, data control, threat protection, and compliance for cloud apps in Microsoft Defender for Cloud Apps documentation.

SASE is also correct because it combines wide-area networking with cloud-delivered security controls such as secure web gateway, CASB, firewall as a service, and zero trust network access. This model is designed to secure access to private/internal applications and external cloud or internet resources using identity- and context-based policy enforcement. Because traffic is steered through a cloud security service edge rather than bypassing inspection through split tunnels, SASE is well aligned with eliminating split-tunnel traffic flows. Gartner's definition of Secure Access Service Edge describes this convergence of networking and security capabilities.

QUESTION NO: 35

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

A. Document interpolation

B. Regular expression pattern matching

C. Optical character recognition functionality

D. Baseline image matching

E. Advanced rasterization

F. Watermarking

ANSWER: B C

Explanation:

Regular expression pattern matching and Optical character recognition functionality are the two capabilities needed for this DLP use case. Regular expression pattern matching lets the DLP engine identify sensitive text patterns in document content, such as account numbers, government identifiers, payment card formats, or other structured data that can be described with pattern logic. This is a core content-inspection method used by DLP and sensitive information type engines to detect protected data at rest. Optical character recognition functionality is also required because the documents include images; without OCR, text embedded in scanned pages, screenshots, or image-based PDF content may not be extracted and analyzed. OCR converts visible characters in images into machine-readable text, allowing the DLP engine to inspect that content using the same detection logic applied to native text. Together, these functions allow the solution to inspect both normal document text and text contained inside images. See Microsoft's guidance on OCR in Microsoft Purview and regular expressions in sensitive information type matching.

QUESTION NO: 36

A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack

B. Privilege escalation attack

C. VPN on the mobile device

D. Unrestricted email administrator accounts

E. Chief use of UDP protocols

F. Disabled GPS on mobile devices

ANSWER: C F

Explanation:

VPN on the mobile device is a likely explanation because geographic access controls commonly evaluate the apparent source location of a connection, especially the public IP address seen by the email service. If a user's phone tunnels traffic through a VPN endpoint located in an approved country or corporate network, the email system may see the login or sync traffic as originating from that permitted location rather than from the user's actual international location. Disabled GPS on mobile devices is also a likely explanation when the organization relies on device location services, mobile device management, or conditional access controls that use location signals from the endpoint. If the phone does not provide usable location data, the control may fail to identify the device as being outside the approved geography, allowing existing mobile email synchronization to continue. In practice, strong location-based access policies should combine trusted network locations, device compliance, session controls, and reauthentication requirements rather than relying on a single signal. Microsoft documents that Conditional Access named locations can be based on IP ranges or countries/regions, and mobile device management platforms can also use device compliance and location-related signals to control access: Microsoft Entra Conditional Access location condition and Microsoft Intune device compliance policies.

QUESTION NO: 37

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

Explanation:

Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall is correct because it separates passive detection from inline prevention in a way that reduces the likelihood of disrupting critical network paths. A NIDS is typically deployed out-of-band using a TAP or switch port mirror/SPAN session so it can inspect copied traffic without being in the forwarding path; if the sensor fails or is overloaded, production traffic can continue flowing. Cisco describes SPAN as a method for copying traffic from one or more ports or VLANs to another port for analysis, which fits this monitoring use case: Cisco SPAN configuration guidance. A NIPS, by contrast, is designed to sit inline so it can actively block malicious traffic, so placing it at a controlled choke point such as the main firewall is a common architecture choice. This allows prevention to be centralized, capacity-planned, monitored, and configured with appropriate availability or fail-open behavior. NIST also distinguishes IDS/IPS sensor placement and notes that inline prevention technologies can affect traffic flow, making placement and design important: NIST SP 800-94.

QUESTION NO: 38

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.

B. Leverage the MITRE ATT&CK framework to map the TTR.

C. Use OSINT techniques to evaluate and analyze the threats.

D. Update security awareness training to address new threats, such as best practices for data security.

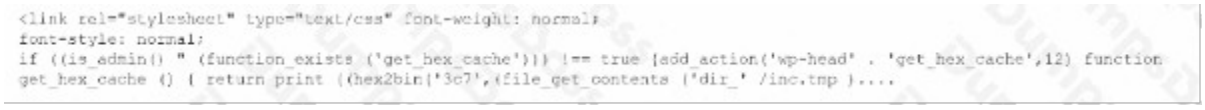
ANSWER: A

Explanation:

Join an information-sharing community that is relevant to the company is the best proactive step because it gives the security engineer access to timely, sector-specific threat intelligence that a small organization may not be able to collect or validate on its own. A company supporting a military program is likely part of, or adjacent to, the defense industrial base, where threats commonly include targeted espionage, intellectual property theft, and nation-state activity. Relevant sharing communities can provide indicators of compromise, adversary tactics, emerging campaign details, mitigation guidance, and peer lessons learned before the company is directly affected. This supports proactive threat management by improving detection content, hardening priorities, incident response preparation, and executive risk decisions based on credible intelligence. Programs such as CISA's information-sharing services and the DoD Defense Industrial Base Cybersecurity Program are designed specifically to help organizations exchange cyber threat information and improve collective defense. See CISA Automated Indicator Sharing and the DoD DIB Cybersecurity Program.

QUESTION NO: 39

A security administrator is reviewing the following code snippet from a website component:



A review of the inc.tmp file shows the following:

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

Explanation:

A content management solution plug-in has been exploited is the most likely cause because the described behavior points to unauthorized code injection in a website component. The code's use of an external temporary file such as inc.tmp, combined with obfuscated or encoded content that is decoded at runtime, is consistent with how attackers hide malicious payloads inside CMS themes, extensions, and plug-ins. In a compromised CMS environment, a vulnerable plug-in can be abused to alter rendered content, metadata, redirects, tracking scripts, or search-engine-facing output, which can lead to visible reporting or indexing inaccuracies. This kind of compromise is especially plausible when the suspicious logic is not part of normal application functionality and relies on hidden files or encoded data to avoid casual review.

CompTIA SecurityX expects candidates to recognize tampering in application components and third-party dependencies as a common web compromise pattern. CMS plug-ins are frequent attack targets because they often run with application-level privileges and may lag behind core platform patching. WordPress specifically recommends reducing attack surface, keeping extensions updated, and reviewing code integrity as part of hardening practices. See WordPress Hardening and OWASP guidance on Vulnerable and Outdated Components.

QUESTION NO: 40

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.

B. Deploy a SIEM.

C. Use containers.

D. Patch the OS

E. Deploy a WAF.

F. Deploy a reverse proxy

G. Deploy an IDS.

ANSWER: A E

Explanation:

Conduct input sanitization is correct because LDAP injection happens when untrusted user input is inserted into LDAP queries without proper validation, escaping, or safe query construction. The most direct remediation is to validate expected input formats and escape LDAP metacharacters before they can alter the logic of an LDAP search filter or distinguished name. OWASP's LDAP Injection Prevention guidance specifically emphasizes escaping variables used in LDAP filters and distinguished names, along with allow-list input validation, as primary defenses: OWASP LDAP Injection Prevention Cheat

Sheet. Deploy a WAF is also correct as a compensating and protective control for an externally exposed application. A properly configured web application firewall can inspect HTTP/S requests, apply rules for injection-style payloads, and block malicious traffic before it reaches the vulnerable application. This is especially useful for reducing exposure while code-level fixes are developed, tested, and deployed. OWASP describes WAFs as controls that monitor, filter, and block HTTP traffic to web applications, often used to mitigate common web application attacks: OWASP Web Application Firewall.

QUESTION NO: 41

Which of the following supports the process of collecting a large pool of behavioral observations to inform decision-making?

A. Linear regression

B. Distributed consensus

C. Big Data

D. Machine learning

ANSWER: C

Explanation:

Big Data is correct because the question is focused on collecting and using a large pool of behavioral observations to support decision-making. In security and enterprise analytics, behavioral observations can include authentication events, endpoint telemetry, network flows, application usage patterns, transaction records, and user activity logs. Big Data platforms and practices are designed to ingest, store, process, and analyze these high-volume, high-velocity, and high-variety datasets so analysts and automated systems can identify trends, detect anomalies, and make better-informed risk or operational decisions. This aligns with the common “3 Vs” model of Big Data: volume, velocity, and variety, which is especially relevant when behavioral data is generated continuously across many users, devices, and systems. The concept is also reflected in formal guidance such as NIST’s Big Data work, which discusses large-scale data characteristics and analytics architectures, and in industry explanations of how Big Data supports insight-driven decisions. See NIST Big Data and IBM: What is big data?.

QUESTION NO: 42

An endpoint security engineer finds that a newly acquired company has a variety of non-standard applications running and no defined ownership for those applications. The engineer needs to find a solution thatrestricts malicious programs and software from running in that environment, while allowing the non-standard applications to function without interruption. Which of the following application control configurations should the engineer apply?

A. Deny list

B. Allow list

C. Audit mode

D. MAC list

ANSWER: A

Explanation:

Deny list is the correct application control configuration because it blocks known malicious, unauthorized, or high-risk software while allowing applications that are not explicitly prohibited to continue running. In a newly acquired environment with many non-standard applications and unclear ownership, this approach minimizes operational disruption because the existing business applications do not need to be fully inventoried, approved, and classified before users can keep working. The engineer can use known indicators such as file hashes, publisher certificates, application names, paths, reputation data, or threat intelligence to prevent confirmed malicious programs from executing while maintaining broad compatibility with the inherited application estate.

This fits the stated requirement: restrict malicious programs and software without interrupting non-standard applications. A deny-list model is commonly used when an organization needs immediate protection but does not yet have enough application governance maturity to safely enforce a strict approved-software-only model. Microsoft describes application control as a way to define what can run, including policies that block untrusted or unwanted code, and NIST also discusses software restriction approaches as part of endpoint protection. See Microsoft App Control for Business and NIST SP 800-167.

QUESTION NO: 43

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.

Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.

B. Implement certificate-based authentication.

C. Verify MD5 hashes.

D. Compress the program with a password.

E. Encrypt with 3DES.

F. Make the DACL read-only.

ANSWER: A F

Explanation:

Utilize code signing by a trusted third party is correct because code signing provides a cryptographic integrity check and establishes publisher authenticity. When each program module is signed, consumers or enforcement controls can validate that the code came from the expected publisher and has not been modified since signing. If a malicious user tampers with a signed executable, library, or script, the signature validation fails, making the alteration detectable and allowing policy-based controls to block execution. Microsoft's code-signing guidance describes this role of digital signatures for verifying software origin and integrity: Microsoft Code Signing.

Make the DACL read-only is also correct because discretionary access control lists are used to define which security principals can read, execute, write, or modify objects such as program files. Configuring the program modules so normal users have read/execute permissions but not write/modify permissions helps prevent unauthorized changes to the deployed code. This complements code signing: permissions reduce the chance of alteration, while signing provides strong tamper detection and trust validation. Microsoft documents how DACLs and access control entries govern access decisions for securable objects: Microsoft DACLs and ACEs.

QUESTION NO: 44

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

Explanation:

Synchronizing all regions* user identities and ensuring ongoing synchronization is correct because the symptoms point to an identity distribution problem created by the move from a unified architecture to a regional federated model. In a federated environment, users may authenticate locally or through trusted regional identity providers, but access decisions still depend on each region having current identity, entitlement, and attribute data. Long-term employees likely benefited because their accounts already existed or were migrated broadly during the initial transition, while new employees may only be provisioned in their home region. When those users travel, remote regions may need to query another region, perform delayed lookups, or fail through slower fallback authentication paths, causing the reported performance issues. The most effective remediation is to ensure identities are synchronized consistently across all regional identity stores and that synchronization continues automatically as employees are hired, changed, or terminated. This aligns with identity federation and lifecycle management best practices described in Microsoft Entra Connect Sync documentation and federation concepts in NIST SP 800-63C.

QUESTION NO: 45

A security analyst is developing a threat model that focuses on attacks associated with the organization ' s storage products. The products:

• Are used in commercial and government user environments

• Are required to comply with crypto-export requirements

• Include both hardware and software components that are developed by external vendors in Europe and Asia

Which of the following are the most important for the analyst to consider when developing the model? (Select two).

A. Contractual obligations

B. Legal hold obligations

C. Trust boundaries

D. Cloud services enumeration

E. Supply chain access

F. Homomorphic encryption usage

ANSWER: C E

Explanation:

Trust boundaries and supply chain access are the most important considerations for this threat model because they directly define where realistic attacks can be introduced and how they can propagate through the storage products. Trust boundaries help the analyst identify where data, commands, firmware updates, cryptographic functions, management interfaces, or administrative privileges cross between components, vendors, customers, and operating environments. For products used by commercial and government customers, those boundaries are especially important because different environments may impose different security assumptions, access controls, cryptographic handling requirements, and assurance expectations. OWASP describes threat modeling as a way to identify what can go wrong in a system and where mitigations are needed, which strongly depends on understanding those boundaries: OWASP Threat Modeling.

Supply chain access is also critical because the products include hardware and software components developed by external vendors in multiple regions. That creates opportunities for compromised components, malicious firmware, vulnerable libraries, tampered build processes, or unauthorized access during development and distribution. NIST emphasizes supply chain risk management as a key discipline for identifying, assessing, and mitigating risks introduced by suppliers, products, and services: NIST SP 800-161r1. For this scenario, modeling supplier access and component trust is essential to anticipating attacks against the storage product ecosystem.

QUESTION NO: 46

An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF

B. XCCDF

C. CPE

D. CVE

E. CVSS

F. OVAL

ANSWER: B F

Explanation:

XCCDF and OVAL are the correct SCAP standards to combine for automated security configuration checking. XCCDF, the Extensible Configuration Checklist Description Format, is designed to express security checklists, benchmarks, profiles, rules, and remediation guidance in a structured XML format. It provides the machine-readable checklist framework that allows best-practice configuration requirements to be organized and selected for assessment. OVAL, the Open Vulnerability and Assessment Language, complements XCCDF by defining the technical tests used to determine whether a system actually satisfies those checklist rules. In practice, an XCCDF benchmark references OVAL definitions so a scanner can automatically evaluate configuration settings, file attributes, registry keys, installed packages, and other system state data. Together, they allow organizations to represent configuration baselines as checklists and automate the collection and evaluation of compliance results across systems. This relationship is central to SCAP-based compliance scanning, as described by NIST's SCAP guidance and the XCCDF specification. See NIST SCAP and NIST XCCDF specification.

QUESTION NO: 47

An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore

B. Embedded cryptoprocessor

C. Hardware-backed public key storage

D. Support for stream ciphers

E. Decentralized key management

F. TPM 2.0 attestation services

ANSWER: B C

Explanation:

Embedded cryptoprocessor and hardware-backed public key storage are the two features that most directly explain why an organization would issue microSD HSMs for remote access. A microSD HSM provides a dedicated hardware security boundary inside a removable form factor, allowing cryptographic operations such as certificate-based authentication, signing, and key exchange to occur inside the device rather than relying only on the mobile operating system. The embedded cryptoprocessor is important because it performs cryptographic functions in hardware and helps protect key material from extraction, malware, and software-level compromise. Hardware-backed public key storage is also central to this use case because remote corporate access commonly depends on PKI credentials, client certificates, and strong device or user authentication. Keeping those keys and credentials in a hardware-backed module increases assurance that authentication secrets remain protected even if the mobile device is lost, rooted, or otherwise compromised. This aligns with the standard purpose of HSMs: secure key generation, storage, and cryptographic processing. See the NIST definition of hardware security module and Android's discussion of hardware-backed keystore protections.

QUESTION NO: 48

A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:

Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

A. Add the objects of concern to the default context.

B. Set the devices to enforcing

C. Create separate domain and context files for irc.

D. Rebuild the policy, reinstall, and test.

ANSWER: B

Explanation:

Set the devices to enforcing is correct because Android's mandatory access control implementation is based on SELinux, and SELinux can operate in permissive or enforcing mode. In permissive mode, SELinux evaluates policy decisions and logs access vector cache denial messages, commonly visible in logs such as dmesg or logcat, but it does not actually block the access. This behavior is intentionally used during policy development and troubleshooting because it allows administrators to see what would have been denied without disrupting device operation. If the analyst sees denial messages but the requested action is still allowed, the policy is most likely being evaluated while the device or relevant domain is permissive. Switching the devices to enforcing causes SELinux to actively enforce the configured MAC policy so denied actions are blocked rather than only logged. Android documentation describes SELinux enforcement as a core Android security feature, and Android source guidance notes the use of permissive mode for testing before enforcing policy. See Android SELinux and Validate SELinux.