



CertsMania

Free Questions for CAS-005

Shared by **Javier** on **Mar 30, 2026**

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

Third parties notified 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?

Options:

- A.
Using IaC to include the newest dependencies
- B.
Creating a bug bounty program
- C.
Implementing a continuous security assessment program
- D.
Integrating a SAST tool as part of the pipeline

Answer

D

Explanation

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. Here's 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.

[References:, CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl,

Questions # 2:

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?

Options:

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

Explanation



CertsMania

Step by Step Explanation:

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

Analyzing the Answer Choices:

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

management.

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

[Reference: This aligns with the principle of applying security controls based on data classification and risk assessment, a key concept in CASP+., C. Begin using cloud-managed keys on all new resources deployed in the cloud: While this would reduce costs, it's a broad approach that doesn't consider the sensitivity of the data. Applying cloud-managed keys to sensitive data might not be acceptable from a security standpoint., D. Extend the key rotation period to one year so that the cloud provider can use cached keys: Extending the key rotation period weakens security. Frequent key rotation is a security best practice to limit the impact of a potential key compromise., Reference: Key rotation is a fundamental security control, and reducing its frequency goes against CASP+ principles related to cryptography and risk management., Why B is the Correct Answer:, Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential., Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper., Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data., CASP+ Relevance: This approach demonstrates an understanding of risk management, data classification, and cost-benefit analysis in security decision-making, all of which are important topics in CASP+., Elaboration on Data Classification:, Data Classification Policy: Organizations should have a clear data classification policy that defines different levels of data sensitivity (e.g., public, internal, confidential, restricted)., Security Controls Based on Classification: Security controls, including encryption key management, should be applied based on the data's classification level., Cost-Benefit Analysis: Data classification helps organizations make informed decisions about where to invest in stronger security controls and where cost optimization is acceptable., In conclusion, adjusting the configuration to use cloud-provider-managed keys for data classified as public is the most effective way to reduce costs while maintaining a strong security posture. It's a practical, risk-based approach that aligns with data classification principles and cost-benefit considerations, all of which are important concepts covered in the CASP+ exam objectives., , , , ,]

Questions # 3:

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?

Options:

A.

SED

B.

eFuse

C.

UEFI

D.

vTPM

E.

MicroSD HSM



CertsMania

Answer

A

Explanation

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. This provides immediate and secure protection if customs agents demand device access, as the sensitive data inside containers becomes unreadable without the decryption key.

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.

Questions # 4:

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?

Options:

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

Explanation

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 is the foundational step.

Option B: Wildcard certificates are for domains, not code signing.

Option C: Recalculating root CA keys is unnecessary and risky unless compromised.

Option D: SAN (Subject Alternative Name) is for multi-domain certificates, irrelevant here.

[Reference: CompTIA SecurityX CAS-005 Domain 2: Security Architecture – PKI Implementation., , , ,]

Questions # 5:

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?

Options:

A.

Performing a port scan

B.

Inspecting egress network traffic

C.

Reviewing the asset inventory

D.

Analyzing user behavior



CertsMania

Answer

C

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 the application 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.

[References:, 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", , , , ,]

Questions # 6:

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 TLS-protected HTTP sessions from systems that do not normally send traffic to

those sites. The technician will define this threat as:

Options:

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.



CertsMania

Answer

C

Explanation

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 an Advanced 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 there's 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 from unusual systems indicates a coordinated, stealthy threat actor.

Option D: An on-path (man-in-the-middle) attack intercepts traffic, but there's no indication of interception; the focus is on unauthorized transfers.

[Reference: CompTIA SecurityX CAS-005 Domain 1: Risk Management – Threat Identification and Analysis., , , ,]

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 controller. The distributed controllers and the shoreside controller communicate over the internet using a cellular network. The company cannot encrypt control traffic because the systems will not tolerate the additional overhead. Which of the following strategies is the best way to reduce the risk of compromise?

Options:

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

D.

Deploying a dedicated base station and reducing the footprint with highly directional antennas

Answer

D

Explanation

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. CompTIA's 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.

[References:, CompTIA SecurityX official exam objectives summary, especially Security Architecture and compensating-control themes.]

Questions # 8:

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?

Options:

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

Explanation

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 doesn't directly address immediate data availability in a DR context.

Option B:Hiring staff supports execution but doesn't define what needs to be recovered or how. It's 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 what's critical ensures the plan meets availability goals efficiently.

[Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations - Disaster Recovery and Business Continuity Planning., , , ,]

Questions # 9:

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?

Options:

A.

Full disk encryption

B.

Remote journaling

C.

Immutable

D.

RAID 10

Answer

B

Explanation

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, , , , , , ,]

Questions # 10:

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

Options:

A.

Risk appetite directly impacts acceptance of high-impact low-likelihood events.

B.

Organizational risk appetite varies from organization to organization

C.

Budgetary pressure drives risk mitigation planning in all companies

D.

Risk appetite directly influences which breaches are disclosed publicly

Answer

A

Explanation

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization ' s risk appetite is crucial because:

It helps prioritize security investments based on the level of risk the organization is willing to tolerate.

High-impact, low-likelihood events may be deemed acceptable if they fall within the organization ' s risk appetite, allowing for budget allocation to other critical areas.

Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization ' s strategic goals.

[References:, CompTIA Security+ Study Guide, NIST Risk Management Framework (RMF) guidelines, ISO 31000, "Risk Management - Guidelines", , , , , ,]

Questions # 11:

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

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

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

Options:

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

Explanation

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

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

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

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

[References:, CompTIA Security+ Study Guide, SANS Institute, "Malware Analysis Techniques", "Practical Malware Analysis" by Michael Sikorski and Andrew Honig, , , , , ,]

Questions # 12:

An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:

1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are

unable to log into the domain from their workstations after relocating to Site B.

2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B

to become inoperable.

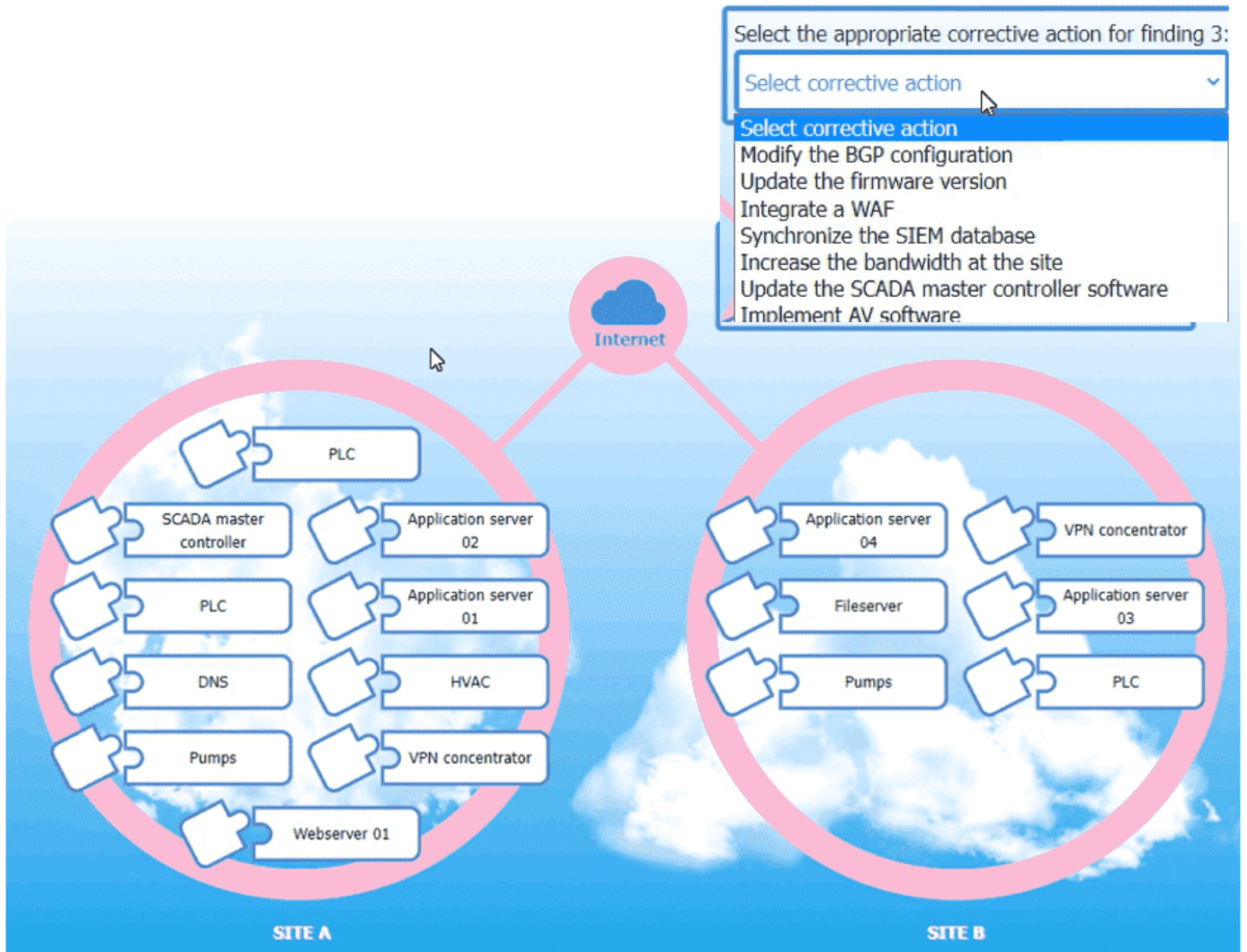
3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet

connectivity at Site B due to route flapping.

INSTRUCTIONS

Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.

For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.



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.

Select this for the item that should be replicated to Site B.

2

A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

Select this for the item that should be replicated to Site B.

3

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

Select this for the item requiring configuration changes.

Options:

Answer

Answer:

See the complete solution below in Explanation:

Explanation



CertsMania

Matching Relevant Findings to the Affected Hosts:

Finding 1:

Affected Host: DNS

Reason: Users are unable to log into the domain from their workstations after relocating to Site B, which implies a failure in domain name services that are critical for user authentication and domain login.

Finding 2:

Affected Host: Pumps

Reason: The pump room at Site B becoming inoperable directly points to the critical infrastructure components associated with pumping operations.

Finding 3:

Affected Host: VPN Concentrator

Reason: Unreliable internet connectivity at Site B due to route flapping indicates issues with network routing, which is often managed by VPN concentrators that handle site-to-site connectivity.

Corrective Actions for Finding 3:

Finding 3 Corrective Action:

Action: Modify the BGP configuration

Reason: Route flapping is often related to issues with Border Gateway Protocol (BGP) configurations. Adjusting BGP settings can stabilize routes and improve internet connectivity reliability.

Replication to Site B for Finding 1:

Affected Host: DNS

Domain Name System (DNS) services are essential for translating domain names into IP

addresses, allowing users to log into the network. Replicating DNS services ensures that even if Site A is disrupted, users at Site B can still authenticate and access necessary resources.

Replication to Site B for Finding 2:

Affected Host: Pumps

The operation of the pump room is crucial for maintaining various functions within the infrastructure. Replicating the control systems and configurations for the pumps at Site B ensures that operations can continue smoothly even if Site A is affected.

Configuration Changes for Finding 3:

Affected Host: VPN Concentrator

Route flapping is a situation where routes become unstable, causing frequent changes in the best path for data to travel. This instability can be mitigated by modifying BGP configurations to ensure more stable routing. VPN concentrators, which manage connections between sites, are typically configured with BGP for optimal routing.

[References: , 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. , , , , , ,]

Questions # 13:

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

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

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

Options:

- 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

Explanation

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

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

Option B delays remediation. Option C overreaches by including Ann in corporate resets.

Option D includes contacting authorities prematurely, which is important but secondary to immediate containment.

CAS-005 emphasizes rapid containment of credential leaks affecting corporate identities, making access resets for John and Joe the first step.

Questions # 14:

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 ' ?

Options:

A.

improving security dashboard visualization on SIEM

B.

Rotating API access and authorization keys every two months

C.

Implementing application load balancing and cross-region availability

D.

Creating WAF policies for relevant programming languages

Answer

D

Explanation

The best way to prevent application-focused attacks for a platform-as-a-service solution with a web-based 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 vulnerabilities and attack patterns.

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

[References:, 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, , , , ,]



CertsMania

To Get Premium Files for CAS-005 Visit

<https://www.certsmania.com/comptia/cas-005-practice>

For More Free Questions Visit

<https://www.certsmania.com/comptia/pdf/cas-005>



CertsMania