



**CertsMania**

## **Free Questions for CAS-005**

**Shared by Eunice on Sep 30, 2025**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**



**CertsMania**

## Questions # 1:

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:

>

Which of the following should the security engineer modify to fix the issue? (Select two).

### Options:

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 srv01 A record must be changed to a type CNAME record pointing to the email server

D.

The email CNAME record must be changed to a type A record pointing to 192.168.1.10

E.

The TXT record must be changed to "v=dkim ip4:192.168.1.11 include my-email.com -ell"

F.

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

G.

The srv01 A record must be changed to a type CNAME record pointing to the web01 server

### Answer

B, D

### Explanation

The security engineer should modify the following to fix the email migration issues:

Email CNAME Record: The email CNAME record must be changed to a type A record

pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.

TXT Record for DMARC: The TXT record must be changed to "v=dmARC ip4:192.168.1.10 include

com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.

DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.

[References:, 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, , , , , ]

## Questions # 2:

Which of the following security risks should be considered as an organization reduces cost and increases availability of services by adopting serverless computing?

### Options:

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

D.

Use of third-party monitoring of service provisioning and configurations

### Answer

A

### Explanation

In serverless computing, organizations rely heavily on CSPs to manage the infrastructure, runtime, and scaling. A key risk is the level 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., , , ]

### Questions # 3:

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

>

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

#### Options:

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

## Explanation

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.

## Questions # 4:

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

### Options:

A.

Securing data transfer between hospitals

B.

Providing for non-repudiation of data

C.

Reducing liability from identity theft

D.

Protecting privacy while supporting portability

## Answer

D

## Explanation

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.", , , , , ]

## Questions # 5:

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?

## Options:

A.

Sigma

B.

YARA

C.

Snort

D.

Rita



CertsMania

## Answer

A

## Explanation

Step-by-Step Explanation:

Sigma (A) is a rule-based detection language that is vendor-agnostic, meaning it can be used across different SIEM (Security Information and Event Management) tools. Unlike YARA (B), which focuses on file-based detection, Sigma provides a standardized way to create rules that work across various security platforms.

## Questions # 6:

An audit finding reveals that a legacy platform has not retained logs for more than 30 days. The platform has been segmented due to its interoperability with newer technology. As a temporary solution, 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?

### Options:

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

### Explanation

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.

[References:, 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., , , , ]

## Questions # 7:

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?

### Options:

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

### Explanation

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.

## Questions # 8:

A security analyst is reviewing a SIEM and generates the following report:

>

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?

### Options:

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

### Explanation

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.

### Questions # 9:

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/Oct/2020 11:24:34 +05:00] "GET /bin/bash" HTTP/1.1" 200 453 Safari/536.36
```

```
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "GET / HTTP/1.1" 200 453 Safari/536.36
```

Application server logs:

```
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
```

```
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing
```

Database server logs:

```
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size1 unassigned value 0 adjusted to 2048
```

```
24/Oct/2020 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?

### Options:

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

## Explanation

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 the X-Forwarded-For header on the load balancer adds the client's 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 doesn't 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 don't help with IP logging.

Option E: Storing `$_SERVER['REMOTE_ADDR']` captures the load balancer's IP, not the client's, unless X-Forwarded-For is enabled.

[Reference: CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations – Log Analysis and Incident Investigation., , , ]

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?

**Options:**

A.

CMDB

B.

Recall tree

C.

ITIL

D.

RACI matrix



CertsMania

**Answer**

D

**Explanation**

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:

“The 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, , , , ]

**Questions # 11:**

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).

**Options:**

A.

CWPP

B.

YAKA

C.

ATTACK

D.

STIX

E.

TAXII

F.

JTAG



CertsMania

**Answer**

D, E

**Explanation**

D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.

E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.

B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.

C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.

F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

[References: , CompTIA Security+ Study Guide, "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE, NIST SP 800-150, "Guide to Cyber Threat Information Sharing", , , , ]

## Questions # 12:

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

### Options:

A.

Software composition analysis

B.

Pre-commit code linting

C.

Repository branch protection

D.

Automated regression testing

E.

Code submit authorization workflow

F.

Pipeline compliance scanning

## Answer

B, D

## Explanation

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

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

Other options:

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

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

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

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

[References: , CompTIA Security+ Study Guide, "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley, OWASP (Open Web Application Security Project) guidelines on secure coding practices, , , , ]

## Questions # 13:

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 of the following best reduces the risk of compromise or sabotage? (Select two).

## Options:

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



CertsMania

## Answer

A, F

## Explanation

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 protect ongoing network communications.

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

[References: , 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, , , , ]

## Questions # 14:

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?

### 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 # 15:

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)
```

Users can specify the document to be parsed by passing the document URL to the application as a parameter. Which of the following is the best solution?

#### Options:

A.

Indexing

B.

Output encoding

C.

Code scanner

D.

Penetration testing

#### Answer

C

#### Explanation

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.", , , ]



CertsMania



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**