



CertsMania

Free Questions for **CAS-005**

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

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

A company's SIEM 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).

Options:

A.

Third-party reports and logs

B.

Trends

C.

Dashboards

D.

Alert failures

E.

Network traffic summaries

F.

Manual review processes

Answer

A, B

Explanation

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 threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false

positives and false negatives.

B. Trends: Analyzing trends over time can help in understanding 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.

[References:, 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., , , ,]

Questions # 2:

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?

Options:

A.

Compliance tracking

B.

Situational awareness

C.

Change management

D.

Quality assurance

Answer

C

Explanation

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.

[References:, CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments., 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., , , ,]

Questions # 3:

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?

Options:

A.

Revoke the user VPN and Wi-Fi certificates

B.

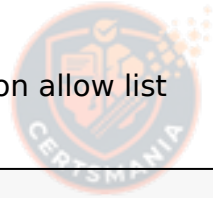
Cryptographically erase FDE volumes

C.

Issue new MFA credentials to all users

D.

Configure the application allow list



CertsMania

Answer

B

Explanation

The key requirement is to instantly eliminate data loss on a lost device.

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

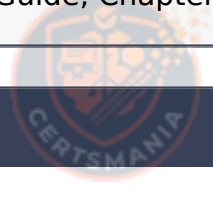
Revoking certificates won't wipe the data from a lost tablet.

Changing MFA credentials won't help unless the device is secured, and app allow lists don't apply post-loss.

From CAS-005, Domain 3: Secure Systems Design and Deployment:

"Cryptographic 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, , , ,]



CertsMania

Questions # 4:

A user reports application access issues to the help desk. The help desk reviews the logs for the user

>

Which of the following is most likely The reason for the issue?

Options:

A.

The user inadvertently tripped the impossible travel security rule in the SSO system.

B.

A threat actor has compromised the user's account and attempted to log in.

C.

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

D.

The user did not attempt to connect from an approved subnet.

Answer

A

Explanation

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

At 8:47 p.m., the user accessed a VPN from Toronto.

At 8:48 p.m., the user accessed email from Los Angeles.

At 8:48 p.m., the user accessed the human resources system from Los Angeles.

At 8:49 p.m., the user accessed email again from Los Angeles.

At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.

[References: , CompTIA SecurityX Study Guide, NIST Special Publication 800-63B, "Digital Identity Guidelines", "Impossible Travel Detection," Microsoft Documentation, , , ,]

Questions # 5:

A global company with a remote workforce implemented a new VPN solution. After deploying the VPN solution to several hundred users, the help desk starts receiving reports of slow access to both internally and externally available applications. A security analyst reviews the following:

VPN client routing: 0.0.0.0/0 → eth1

Which of the following solutions should the analyst use to fix this issue?

Options:

A.

Move the servers to a screened subnet.

B.

Enable split tunneling.

C.

Configure an NAC solution.

D.

Implement DNS over HTTPS.

Answer

B

Explanation

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.

Questions # 6:

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

>

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

Options:

A.

An endpoint that is not submitting any logs

B.

Potential activity indicating an attacker moving laterally in the network

C.

A misconfigured syslog server creating false negatives

D.

Unauthorized usage attempts of the administrator account

Answer

D

Explanation

Understanding the Security Event:

Administrator accounts are highly privileged and require strict monitoring.

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

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

Why Option D is Correct:

Failed logins for administrator accounts are a critical security concern.

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

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

Why Other Options Are Incorrect:

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

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

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

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

Questions # 7:

A user reports application access issues to the help desk. The help desk reviews the logs for the user:

>

Which of the following is most likely the reason for the issue?

Options:

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

Explanation

The logs show that the user connected from Toronto (104.18.16.29) and Los Angeles (95.67.137.12) within minutes. The sudden location change is a typical trigger for geoblocking in a Next-Generation Firewall (NGFW), leading to the HR 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 on Firewall Rules and Network Traffic Analysis, , ,]

Questions # 8:

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

Options:

- 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

Explanation

Step by Step Explanation:

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

Analyzing the Answer Choices:

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

[Reference: 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., Why A is the Correct Answer:, Air Gap: The concept of an air gap (physical isolation) was the cornerstone of security for many legacy OT systems. These systems were not connected to the internet or corporate networks, making them less susceptible to remote attacks., Legacy Protocols: Older OT systems often used proprietary or serial communication protocols, not designed for internet connectivity., Implicit Trust: Within the isolated environment, there was often an assumption of trust among the connected components., CASP+ Relevance: The challenges of securing legacy OT systems, especially in the face of increasing connectivity, are a key area of focus in CASP+. Understanding the historical context and the shift in security paradigms is crucial., Modern OT Security Considerations (Elaboration):, Convergence: Today, the lines between IT and OT are blurring. OT systems are increasingly connected to corporate networks and the internet, necessitating a shift from isolation-based security to a more comprehensive approach., Threat Landscape: Modern OT systems face a wider range of threats, including targeted attacks from sophisticated actors., Security Controls: Modern OT security involves implementing network segmentation, intrusion detection, access controls, and other measures to protect against these evolving threats., In conclusion, the primary design assumption for many older OT systems was that they

would operate in isolated or disconnected environments. This historical context is important for understanding the security challenges faced by organizations today as they integrate these legacy systems into modern, connected environments. This is a core concept discussed in CASP+ in the context of OT security and risk management.,
=====, , ,]

Questions # 9:

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?

Options:

A.

SOAR

B.

CWPP

C.

XCCDF

D.

CMDB

Answer

A

Explanation

Integrating IDS, firewall, and DLP to reduce response time requires orchestration and automation. Let's evaluate:

A. SOAR(Security Orchestration, Automation, and Response):SOAR integrates security tools, automates workflows, and speeds up incident response. It's the best fit for this scenario, as CAS-005 highlights SOAR for operational efficiency.

B. CWPP (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., , , ,]

Questions # 10:

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., , ,]



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