CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct 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.

References:

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

ITIL (Information Technology 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 2

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

D. Credentialed vulnerability scan

Correct Answer: B

A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a

private 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

vulnerability management:

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. References: CompTIA SecurityX Study Guide "Software Bill of Materials (SBoM)," NIST Documentation "Managing Container Security with SBoM," OWASP

QUESTION 3

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

D. The retention policy is not property configured

Correct Answer: 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 the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

QUESTION 4

An organization developed a containerized application. The organization wants to run the application in the cloud and automatically scale it based on demand. The security operations team would like to use container orchestration but does not want to assume patching responsibilities. Which of the following service models best meets these requirements?

A. PaaS

B. SaaS

C. IaaS

D. MaaS

Correct Answer: A

QUESTION 5

Before launching a new web application, an organization would like to perform security testing. Which of the following resources should the organization use to determine the objectives for the test?

A. CASB

B. SOAR

C. OWASP

D. ISAC

Correct Answer: C