# Free PDF Quiz 2026 CompTIA CAS-005: CompTIA SecurityX Certification Exam First-grade Dumps Guide


2026 Latest DumpsFree CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: https://drive.google.com/open?id=1IEVyA7FnUmOGMgVY7Sqj85mHKgImstdW

If you have a faith, then go to defend it. Gorky once said that faith is a great emotion, a creative force. My dream is to become a top IT expert. I think that for me is nowhere in sight. But to succeed you can have a shortcut, as long as you make the right choice. I took advantage of DumpsFree's CompTIA CAS-005 exam training materials, and passed the CompTIA CAS-005 Exam. DumpsFree CompTIA CAS-005 exam training materials is the best training materials. If you're also have an IT dream. Then go to buy DumpsFree's CompTIA CAS-005 exam training materials, it will help you achieve your dreams.

## CompTIA CAS-005 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security. |
| Topic 2 | • Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems. |
| Topic 3 | • Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems. |
| Topic 4 | • Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering. |

**>> Dumps CAS-005 Guide <<**

## CAS-005 Valid Test Question - CAS-005 Exam Simulator Fee

As is known to us, there are best sale and after-sale service of the CAS-005 certification training dumps all over the world in our company. Our company has employed a lot of excellent experts and professors in the field in the past years, in order to design the

best and most suitable CAS-005 latest questions for all customers. More importantly, it is evident to all that the CAS-005 Training Materials from our company have a high quality, and we can make sure that the quality of our products will be higher than other study materials in the market. If you want to pass the CAS-005 exam and get the related certification in the shortest time, choosing the CAS-005 training materials from our company will be in the best interests of all people.

## CompTIA SecurityX Certification Exam Sample Questions (Q49-Q54):

**NEW QUESTION # 49**
After an incident response exercise, a security administrator reviews the following table:
Which of the following should the administrator do to beat support rapid incident response in the future?

- A. Configure automated Isolation of human resources systems
- B. Enable dashboards for service status monitoring
- C. Automate alerting to IT support for phone system outages.
- D. Send emails for failed log-In attempts on the public website

**Answer: B**

Explanation:
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.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"
"Best Practices for Implementing Dashboards," Gartner Research

**NEW QUESTION # 50**

**Answer:**

Explanation:
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.

**NEW QUESTION # 51**
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. Perform security awareness training focusing on phishing.
- B. Enforce email encryption standards.
- C. Create an acceptable use policy.
- D. Automatically quarantine outgoing email.

**Answer: C**

Explanation:
An acceptable 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.

**NEW QUESTION # 52**
A company's 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:
Which of the following accounts should a security analyst disable to best contain the incident without impacting valid users?

- A. user-d
- B. user-a
- C. user-c
- D. user-b

**Answer: C**

Explanation:
User user-c is showing anomalous 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) and user-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-c's pattern is more consistent with an attack technique.

**NEW QUESTION # 53**
Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:
* Full disk encryption
* Host-based firewall
* Time synchronization
* Password policies
* Application allow listing
* Zero Trust application access
Which of the following solutions best addresses the requirements? (Select two).

- A. SBoM
- B. SCAP
- C. SASE
- D. HIDS
- E. CASB

**Answer: B,C**

Explanation:
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.
References:
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 maintained effectively.

**NEW QUESTION # 54**
.....

You will receive a registration code and download instructions via email. We will be happy to assist you with any questions regarding our products. Our CompTIA SecurityX Certification Exam (CAS-005) practice exam software helps to prepare applicants to practice time management, problem-solving, and all other tasks on the standardized exam and lets them check their scores. The CompTIA SecurityX Certification Exam (CAS-005) practice test results help students to evaluate their performance and determine their readiness without difficulty.



P.S. Free 2026 CompTIA CAS-005 dumps are available on Google Drive shared by DumpsFree: https://drive.google.com/open?id=1IEVyA7FnUmOGMgVY7Sqj85mHKgImstdW