

# The Ideal Solution for CompTIA CAS-005 Exam Questions Preparation



DOWNLOAD the newest ValidExam CAS-005 PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1\\_xvVLnLGK4z1LqUPQCxl\\_OLibFr27Tt](https://drive.google.com/open?id=1_xvVLnLGK4z1LqUPQCxl_OLibFr27Tt)

All these features make the CAS-005 exam practice question the ideal study material for CAS-005 exam preparation and it is designed to assist you in CompTIA SecurityX Certification Exam (CAS-005) practice test. We guarantee you that you will not find all these top-rated features anywhere. They are only available with CAS-005 exam questions format.

## CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>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.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>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.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>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.</li></ul>

>> Exam CAS-005 Reference <<

**CAS-005 – 100% Free Exam Reference | the Best Test CompTIA SecurityX**

# Certification Exam Study Guide

Our CAS-005 preparation questions deserve you to have a try. As long as you free download the demos on our website, then you will love our CAS-005 preparation braindumps for its high quality and efficiency. All you have learned on our CAS-005 Study Materials will play an important role in your practice. We really want to help you solve all your troubles about learning the CAS-005 exam. Please give us a chance to prove.

## CompTIA SecurityX Certification Exam Sample Questions (Q202-Q207):

### NEW QUESTION # 202

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?

- A. Design an appropriate warm site for business continuity.
- B. Hire additional on-call staff to be deployed if an event occurs.
- C. Implement a change management plan to ensure systems are using the appropriate versions.
- **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.

### NEW QUESTION # 203

A vulnerability scan was performed on a website, and the following encryption suites were found:  
Which of the following actions will remediate the vulnerability?

- A. Reissuing new SSL certificates for the website
- **B. Removing any ciphers utilizing cipher block chaining**
- C. Rearranging the order of the ciphers from strongest to weakest
- D. Deploying a WAF to monitor web traffic

**Answer: B**

### NEW QUESTION # 204

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- \* 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. SASE**
- **B. SCAP**
- C. SBoM

- D. CASB
- E. HIDS

**Answer: A,B**

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 # 205

A software engineer is creating a CI/CD pipeline to support the development of a web application. The DevSecOps team is required to identify syntax errors. Which of the following is the most relevant to the DevSecOps team's task?

- A. Software composition analysis
- B. Runtime application self-protection
- **C. Static application security testing**
- D. Web application vulnerability scanning

**Answer: C**

Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

A: Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.

B: Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.

C: Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.

D: Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

### NEW QUESTION # 206

A security architect wants to develop a baseline of security configurations. These configurations automatically will be utilized machine is created. Which of the following technologies should the security architect deploy to accomplish this goal?

- A. Short
- **B. Ansible**
- C. GASB
- D. CMDB

**Answer: B**

To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Here's why:

Automation: Ansible is an automation tool that allows for the configuration, management, and deployment of applications and systems. It ensures that security configurations are consistently applied across all new machines.

**Scalability:** Ansible can scale to manage thousands of machines, making it suitable for large enterprises that need to maintain consistent security configurations across their infrastructure.

**Compliance:** By using Ansible, organizations can enforce compliance with security policies and standards, ensuring that all systems are configured according to best practices.

### NEW QUESTION # 207

• • • • •

Our CAS-005 exam questions provide with the software which has a variety of self-study and self-assessment functions to detect learning results. The statistical reporting function is provided to help students find weak points and deal with them. Our software is also equipped with many new functions, such as timed and simulated test functions. After you set up the simulation test timer with our CAS-005 Test Guide which can adjust speed and stay alert, you can devote your mind to learn the knowledge. There is no doubt that the function can help you pass the CAS-005 exam.

**Test CAS-005 Study Guide:** <https://www.validexam.com/CAS-005-latest-dumps.html>

- [illegible]

What's more, part of that ValidExam CAS-005 dumps now are free: [https://drive.google.com/open?id=1\\_xvVLnGK4zILqUPOCxl\\_OLibFr27Tt](https://drive.google.com/open?id=1_xvVLnGK4zILqUPOCxl_OLibFr27Tt)