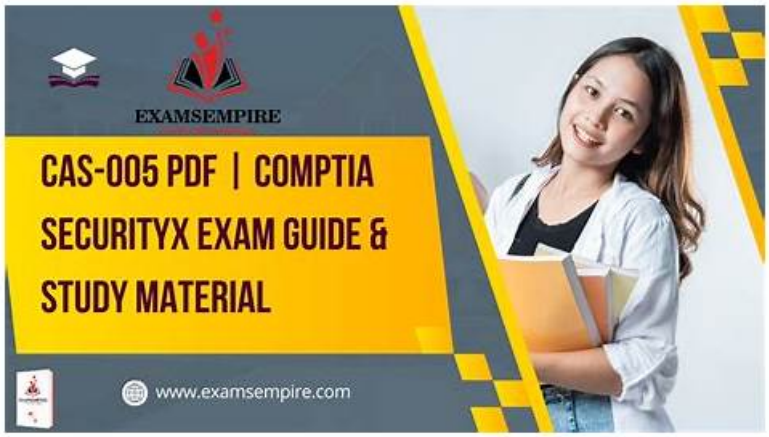
CAS-005 Exam Reviews - New CAS-005 Study Plan



2025 Latest PDF4Test CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: https://drive.google.com/open?id=1GCgZQRT5fzhcC2h_1JaGxE8PkzjGonql

Our product is revised and updated according to the change of the syllabus and the latest development situation in the theory and the practice. The CAS-005 Exam Torrent is compiled elaborately by the experienced professionals and of high quality. The contents of CAS-005 guide questions are easy to master and simplify the important information. It conveys more important information with less answers and questions, thus the learning is easy and efficient. The language is easy to be understood makes any learners have no obstacles.

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 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 3	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection 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.

>> CAS-005 Exam Reviews <<

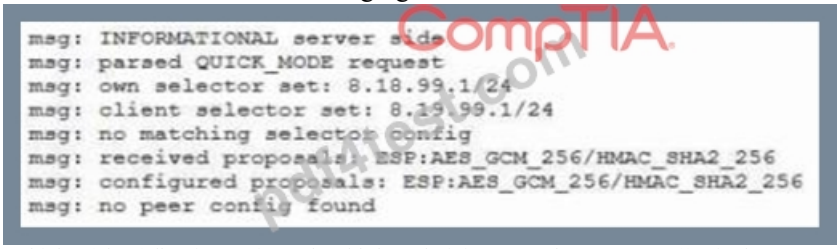
New CAS-005 Study Plan & Exam CAS-005 Bootcamp

Our practice exams are designed solely to help you get your CompTIA CAS-005 certification on your first try. A CompTIA CAS-005 practice test will help you understand the exam inside out and you will get better marks overall. It is only because you have practical experience of the exam even before the exam itself. PDF4Test offers authentic and up-to-date study material that every candidate can rely on for good preparation. Our top priority is to help you pass the CompTIA SecurityX Certification Exam (CAS-

005) exam on the first try.

CompTIA SecurityX Certification Exam Sample Questions (Q285-Q290):

NEW QUESTION # 285
An administrator reviews the following log and determines the root cause of a site-to-site tunnel failure:



Which of the following actions should the administrator take to most effectively correct the failure?

- A. Enable perfect forward secrecy on the remote peer.
- B. Update the cipher suites configured for use on the server side.
- C. Add a new subnet as a permitted initiator.
- D. Disable IKE version 1 and run IKE version 2.

Answer: C

NEW QUESTION # 286
Emails that the marketing department is sending to customers are pomp to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three.)

- A. DNSSEC
- B. SASC
- C. DKIM
- D. SAN
- E. DMARC
- F. SOA
- G. MX
- H. SPF

Answer: C,E,H

Explanation:
To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server's certificates:
* A. DMARC (Domain-based Message Authentication, Reporting & Conformance): DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.
* B. SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.
* C. DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to email headers, allowing the receiving server to verify that the email has not been tampered with and is from an authorized sender.
Updating DKIM records ensures that emails are properly signed and authenticated.
* D. DNSSEC (Domain Name System Security Extensions): DNSSEC adds security to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam.
* E. SASC: This is not a relevant standard for this scenario.
* F. SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues.
* G. SOA (Start of Authority): SOA records are used for DNS zone administration and do not directly impact email deliverability.
* H. MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which is handled by SPF, DKIM, and DMARC.
References:
* CompTIA Security+ Study Guide

* RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC)
* NIST SP 800-45, "Guidelines on Electronic Mail Security"

NEW QUESTION # 287
The material finding from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep.
Which of the following solutions are the best ways to mitigate this issue? (Select two).
Setting different access controls defined by business area

- A. Implementing a role-based access policy
- B. Establishing a mandatory vacation policy
- C. Requiring periodic job rotation
- D. Designing a least-needed privilege policy
- E. Performing periodic access reviews

Answer: A,E

Explanation:
To mitigate the issue of excessive permissions and privilege creep, the best solutions are:
* Implementing a Role-Based Access Policy:
* Role-Based Access Control (RBAC): This policy ensures that access permissions are granted based on the user's role within the organization, aligning with the principle of least privilege.
Users are only granted access necessary for their role, reducing the risk of excessive permissions.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations
* Performing Periodic Access Reviews:
* Regular Audits: Periodic access reviews help identify and rectify instances of privilege creep by ensuring that users' access permissions are appropriate for their current roles. These reviews can highlight unnecessary or outdated permissions, allowing for timely adjustments.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* ISO/IEC 27001:2013 - Information Security Management

NEW QUESTION # 288
A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution
Which of the following most likely explains the choice to use a proxy-based CASB?

- A. Privacy compliance obligations are bypassed when using a user-based deployment.
- B. Protecting and regularly rotating API secret keys requires a significant time commitment
- C. Corporate devices cannot receive certificates when not connected to on-premises devices
- D. The capability to block unapproved applications and services is possible

Answer: D

Explanation:
A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:
* Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.
* Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.
* Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies
* Gartner CASB Market Guide

NEW QUESTION # 289
A security architect is performing threat-modeling activities related to an acquired overseas software company that will be integrated with existing products and systems Once its software is integrated, the software company will process customer data for the acqumng company Given the following:

ID	Threat	STRIDE	Criticality
01	Attacker performs denial of service against public-facing endpoints	Denial of service	High
02	Malicious insider puts a backdoor into source code	Tampering	Critical
03	Attacker injects malicious code into third-party library	Tampering	Critical
04	Attacker escalates privilege to administrator in web system	Elevation of privilege	High
05	Attacker performs successful password spraying	Spoofing	High

Which of the following mitigations would reduce the risk of the most significant threats?

- A. Zero Trust architecture for all assets from the acquired company using microsegmentation against sensitive applications
- B. Rate-limiting capabilities on all authentication systems and leveraging single sign-on through federation
- C. Privileged access management system with conditional access capabilities to prevent unauthorized access
- D. Secure development process with gate checks and appropriate code scanning

Answer: D

Explanation:
The table highlights that tampering threats (IDs 02 and 03) are rated Critical, making them the most significant risks. These threats involve malicious insiders inserting backdoors or attackers injecting malicious code into third-party libraries. To mitigate such risks, organizations must implement a secure software development lifecycle (SDLC) with formalized code scanning, gate checks, and supply chain validation.
Option C directly addresses these issues. Secure development practices include static/dynamic code analysis, dependency checks, peer reviews, and mandatory approvals before code promotion. This approach detects backdoors, prevents unauthorized modifications, and reduces the likelihood of compromised libraries being integrated.
Option A (PAM with conditional access) mitigates privilege escalation but does not address software tampering. Option B (rate limiting and federation) reduces brute-force authentication risks (ID 05) but not critical tampering. Option D (Zero Trust with microsegmentation) strengthens network defense but does not secure the integrity of source code or libraries.

NEW QUESTION # 290
.....

- CAS-005 - Professional CompTIA SecurityX Certification Exam Exam Reviews □ Search for 「 CAS-005 」 and obtain a free download on ▹ www.pdfvce.com ◃ □Free CAS-005 Study Material
- Free PDF Quiz Newest CompTIA - CAS-005 - CompTIA SecurityX Certification Exam Exam Reviews □ Search for 「 CAS-005 」 and obtain a free download on { www.practicevce.com } □CAS-005 Exam Vce
- High Hit-Rate CAS-005 Exam Reviews | 100% Free New CAS-005 Study Plan □ Search for ➽ CAS-005 □ and download it for free on ▸ www.pdfvce.com ◂ website □Pass CAS-005 Guide
- Study CAS-005 Material □ Latest CAS-005 Dumps Ebook □ CAS-005 Study Demo □ Search for [CAS-005] and easily obtain a free download on ▹ www.troytecdumps.com ◃ □PDF CAS-005 Download
- PDF CAS-005 Download □ Pass CAS-005 Guide □ Latest CAS-005 Braindumps Files □ Open website □ www.pdfvce.com □ and search for ➤ CAS-005 □ for free download □CAS-005 Study Demo
- Trustable CAS-005 – 100% Free Exam Reviews | New CAS-005 Study Plan □ ➽ www.exam4labs.com □ is best website to obtain ➥ CAS-005 □ for free download □Exam CAS-005 Material
- Latest CAS-005 Dumps Ebook □ CAS-005 Exam Vce □ Exam CAS-005 Material □ Download ➡ CAS-005 □□□ for free by simply entering □ www.pdfvce.com □ website □Valid Exam CAS-005 Registration
- 2026 High Hit-Rate CAS-005 – 100% Free Exam Reviews | New CompTIA SecurityX Certification Exam Study Plan □ The page for free download of □ CAS-005 □ on 《 www.torrentvce.com 》 will open immediately □Reliable CAS-005 Test Pass4sure
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, study.stcs.edu.np, Disposable vapes

DOWNLOAD the newest PDF4Test CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1GCgZQRT5fzhcC2h_1JaGxE8PkzjGonq1