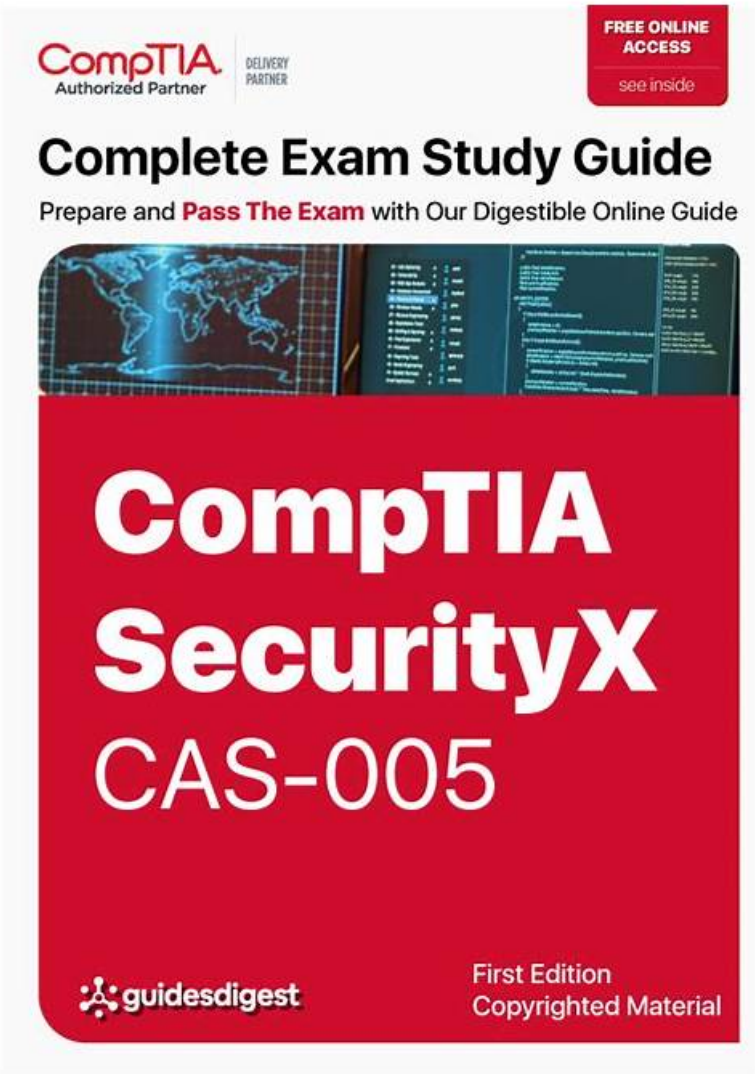
CompTIA - CAS-005 Perfect Valid Test Discount



DOWNLOAD the newest PDFDumps CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1BjtZ6mAGZO6xZ_azwwC-Mn0Plg3FdDTw

There are a lot of excellent experts and professors in our company. The high quality of the CAS-005 reference guide from our company resulted from their constant practice, hard work and their strong team spirit. After a long period of research and development, our CAS-005 test questions have been the leader study materials in the field. We have taken our customers' suggestions of the CAS-005 Exam Prep seriously, and according to these useful suggestions, we have tried our best to perfect the CAS-005 reference guide from our company just in order to meet the need of these customers well. So stop hesitation and buy our study materials.

May be you doubt the ability of our CompTIA test dump; you can download the trial of our practice questions. All CAS-005 exam prep created by our experienced IT workers who are specialized in the certification study guide. We checked the updating of CAS-005 vce braindumps to make sure the preparation successful.

>> Valid CAS-005 Test Discount <<

Hot Valid CAS-005 Test Discount | Efficient CAS-005 Cert Exam: CompTIA SecurityX Certification Exam

The latest CompTIA SecurityX Certification Exam CAS-005 exam and exam study guide is reliable, CompTIA SecurityX

Certification Exam CAS-005 with reasonable exam price and guaranteed questions answers. CompTIA offers actual CompTIA SecurityX Certification Exam to sure your success in CAS-005 Exam. Don't worry, this CompTIA SecurityX Certification Exam CAS-005 test price is benefit and content is 365 days updates!

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	• 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.
Topic 4	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

CompTIA SecurityX Certification Exam Sample Questions (Q196-Q201):

NEW QUESTION # 196
A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points

User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr0ll.com	GET	Blocked	Blocked	No
account2	p4yr0ll.com	POST	Blocked	Blocked	No
account2	139.40.20.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

- A. utilizing allow lists on the WAF for all users using GFT methods
- B. Adjusting the SIEM to alert on attempts to visit phishing sites
- C. Allowing TRACE method traffic to enable better log correlation
- D. Enabling alerting on all suspicious administrator behavior

Answer: D

Explanation:
In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here's a detailed analysis of the options provided:
A: Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn't directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
B: Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It's not typically recommended for enhancing security monitoring or incident response.
C: Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell time significantly. Suspicious behavior

could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns.
This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
D: Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn't specifically address the need for quick detection and response to internal threats.
References:
CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
NIST Special Publication 800-61 Revision 2,"Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
"Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia:
Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.
Top of Form
Bottom of Form

NEW QUESTION # 197
A security architect must make sure that the least number of services as possible is exposed in order to limit an adversary's ability to access the systems. Which of the following should the architect do first?

- A. Perform attack surface reduction.
- B. Enforce Secure Boot.
- C. Limit access to the systems.
- D. Disable third-party integrations.

Answer: A

Explanation:
Attack surface reduction focuses on minimizing unnecessary services, open ports, and vulnerabilities, reducing the exposure to potential adversaries. This aligns with zero trust and least privilege principles.
* Secure Boot (A) helps ensure system integrity but does not minimize exposed services.
* Disabling third-party integrations (C) may help, but broader attack surface reduction is the best first step.
* Limiting access (D) is important but does not directly reduce exposed services.

NEW QUESTION # 198
PKI can be used to support security requirements in the change management process. Which of the following capabilities does PKI provide for messages?

- A. Non-repudiation
- B. Confidentiality
- C. Delivery receipts
- D. Attestation

Answer: A

Explanation:
Public Key Infrastructure (PKI) supports change management by securing messages (e.g., approvals, updates).
Non-repudiation, provided via digital signatures, ensures a sender cannot deny sending a message, critical for auditability in change processes.
* Option A:Correct-PKI's digital signatures ensure non-repudiation.
* Option B:Confidentiality (via encryption) is a PKI feature but less tied to change management's focus on accountability.
* Option C:Delivery receipts are not a PKI function; they're protocol-specific (e.g., SMTP).
* Option D:Attestation relates to verifying attributes, not a direct PKI message capability.

NEW QUESTION # 199
A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:
Error Message in Database Connection
Connection to host USA-WebApp-Database failed
Database "Prod-DB01" not found
Table "CustomerInfo" not found
Please retry your request later
Which of the following best describes the analyst's findings and a potential mitigation technique?

- A. The findings indicate a SQL injection. The database needs to be upgraded.
- B. The findings indicate unsecure references. All potential user input needs to be properly sanitized.
- C. The findings indicate unsecure protocols. All cookies should be marked as HttpOnly.
- D. The findings indicate information disclosure. The displayed error message should be modified.

Answer: D

Explanation:
The error message reveals sensitive details (hostnames, database names, table names), constituting information disclosure. This aids attackers in reconnaissance. Mitigation involves modifying the application to display generic error messages (e.g., "An error occurred") instead of specifics.
* Option A:Unsecure references suggest coding flaws, but this is a configuration/output issue, not input sanitization.
* Option B:Unsecure protocols and HttpOnly cookies relate to session security, not error handling.
* Option C:Correct-information disclosure is the issue; generic errors mitigate it.
* Option D:No evidence of SQL injection (e.g., manipulated input); upgrading the database doesn't address disclosure.

NEW QUESTION # 200
A user tried to access a web page at http://10.1.1.1. Previously the web page did not require authentication, and now the browser is prompting for credentials. Which of the following actions would best prevent the issue from reoccurring and reduce the likelihood of credential exposure?

- A. Modifying web server configuration and utilizing X509 certificates forauthentication
- B. Installing new rules for the IDS to detect impersonation attacks
- C. Transitioning internal services to use DNS security
- D. Implementing 802.1x EAP-TTLS on access points to reduce the risk of evil twins

Answer: A

NEW QUESTION # 201
.....

□ www.pdfvce.com □ enter ➥ CAS-005 □ and obtain a free download □CAS-005 Valid Dumps

- Latest CAS-005 Real Exam Questions, CompTIA CAS-005 Practice Test, CompTIA SecurityX Certification Exam □ Easily obtain free download of ☀ CAS-005 □☀□ by searching on 【 www.testkingpass.com 】 □CAS-005 Latest Test Practice
- Relevant CAS-005 Exam Dumps □ CAS-005 Braindumps Torrent □ New CAS-005 Test Simulator □ Search on ▸ www.pdfvce.com ◂ for □ CAS-005 □ to obtain exam materials for free download □Latest CAS-005 Guide Files
- Updated Valid CAS-005 Test Discount - Trustable CAS-005 Cert Exam - Hot CompTIA CompTIA SecurityX Certification Exam □ Download { CAS-005 } for free by simply entering 「 www.verifieddumps.com 」 website □ □Reliable CAS-005 Exam Review
- CAS-005 Valid Dumps □ CAS-005 Reliable Test Voucher □ CAS-005 Valid Dumps □ Go to website □ www.pdfvce.com □ open and search for ➥ CAS-005 □ to download for free □New CAS-005 Test Simulator
- Latest CAS-005 Real Exam Questions, CompTIA CAS-005 Practice Test, CompTIA SecurityX Certification Exam □ Copy URL ➥ www.pass4test.com □ open and search for { CAS-005 } to download for free □New CAS-005 Exam Topics
- harleyzzra464150.muzwiki.com, nelsonpvqv716732.fare-blog.com, lewysceli985875.kylieblog.com, lewysonad725482.blognody.com, jemimaztcn827468.wikiadvocate.com, donnamizu048830.csublogs.com, jakubttpg799348.shoutmyblog.com, www.teachmenow.eu, 1001bookmarks.com, minibookmarking.com, Disposable vapes

2026 Latest PDFDumps CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: https://drive.google.com/open?id=1BjtZ6mAGZO6xZ_azwwC-Mn0Plg3FdDTw