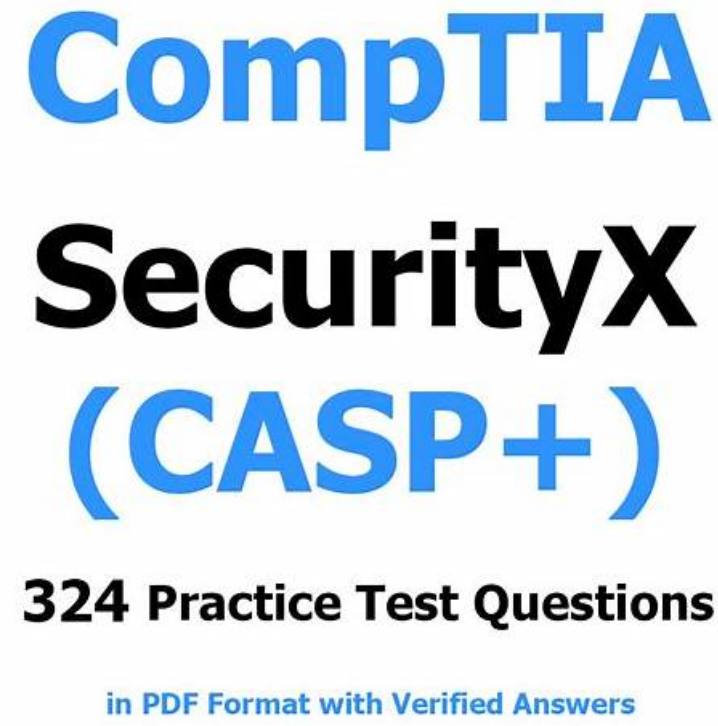
Free CompTIA CAS-005 Practice & CAS-005 Latest Test Materials



P.S. Free & New CAS-005 dumps are available on Google Drive shared by Dumpcollection: https://drive.google.com/open?id=1uT-W6f0mHkDvSWo9OfNUu64Kv9_sMbw5

Get the test CAS-005 certification requires the user to have extremely high concentration will all test sites in mind, and this is definitely a very difficult. Our CAS-005 learning questions can successfully solve this question for you for the content are exactly close to the changes of the CAS-005 Real Exam. When you grasp the key points, nothing will be difficult for you anymore. Our professional experts are good at compiling the CAS-005 training guide with the most important information. Believe in us, and your success is 100% guaranteed!

The information technology market has become very competitive. CompTIA CAS-005 technologies and services are constantly evolving. Therefore, the CompTIA CAS-005 certification has become very important to advance one's career. Success in the CompTIA SecurityX Certification Exam CAS-005 exam validates and upgrades your skills in CompTIA CAS-005 technologies. It is the main reason behind the popularity of the CompTIA CAS-005 certification exam. You must put all your efforts to clear the challenging CompTIA CAS-005 examination. However, cracking the CAS-005 test is not an easy task.

>> Free CompTIA CAS-005 Practice <<

Golden Opportunity to Get a 50% Discount on CompTIA CAS-005 PDF Questions with 365 days Free Updates

Dumpcollection makes your CAS-005 exam preparation easy with it various quality features. Our CAS-005 exam braindumps come with 100% passing and refund guarantee. Dumpcollection is dedicated to your accomplishment, hence assures you successful in CAS-005 Certification exam on the first try. If for any reason, a candidate fails in CAS-005 exam then he will be refunded his money after the refund process. Also, we offer 1 year free updates to our CAS-005 Exam esteemed user, these updates are applicable to your account right from the date of purchase. 24/7 customer support is favorable to candidates who can email us if they find any ambiguity in the CAS-005 exam dumps, our support will merely reply to your all CAS-005 exam product related queries.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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.

CompTIA SecurityX Certification Exam Sample Questions (Q523-Q528):

NEW QUESTION # 523
A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user:
Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

Answer: B

Explanation:
The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non- business hours, reducing the risk of security incidents.

NEW QUESTION # 524
A security analyst is reviewing the following authentication logs:
Which of the following should the analyst do first?

- A. Disable User12's account
- B. Disable User1's account
- C. Disable User2's account
- D. Disable User8's account

Answer: B

Explanation:
Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here's a breakdown of why disabling User1's account is the appropriate first step:
* Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:
* VM01 at 8:01:23 AM

* VM08 at 8:01:23 AM
* VM01 at 8:01:23 AM
* VM08 at 8:01:23 AM
* Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.
* Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* CompTIA Security+ Certification Exam Objectives
* NIST Special Publication 800-63B: Digital Identity Guidelines
By addressing User1's account first, we effectively mitigate the immediate threat of a brute-force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

NEW QUESTION # 525
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. Ansible
- B. GASB
- C. Short
- D. CMDB

Answer: A

Explanation:
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.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
Ansible Documentation: Best Practices
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

NEW QUESTION # 526
A company experienced a data breach, resulting in the disclosure of extremely sensitive data regarding a merger. As a regulated entity, the company must comply with reporting and disclosure requirements. The company is concerned about its public image and shareholder values. Which of the following best supports the organization in addressing its concerns?

- A. Supply chain management program
- B. Data subject access request
- C. Business impact analysis
- D. Crisis management plan

Answer: D

Explanation:
A crisis management plan defines coordinated communication and response strategies for high-profile incidents that may harm an organization's public reputation and shareholder confidence. CAS-005 GRC content includes crisis communication planning for regulatory compliance and public relations in the wake of breaches.
A Data Subject Access Request (A) addresses individual data rights, not overall crisis handling.
Business Impact Analysis (B) helps assess potential operational and financial impacts but does not manage public perception during

an incident.

NEW QUESTION # 527
A company'sSIEMis designed to associate the company'sasset inventorywith user events. Given the following report:
Which of the following should asecurity engineer investigate firstas part of alog audit?

- A. Amisconfigured syslog servercreating false negatives
- B. Unauthorized usage attempts of the administrator account
- C. Potential activity indicating an attackermoving laterally in the network
- D. Anendpointthat is not submitting any logs

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
* Understanding the Security Event:
* Administrator accounts are highly privilegedand require strict monitoring.
* Server 4 shows failed login attempts for the administrator account.This could indicate a brute-force attack or unauthorized access attempt.
* The fact thatnone of the admin login attempts were successfulsuggestssomeone was trying to guess the credentials.
* Why Option D is Correct:
* Failed logins for administrator accounts are a critical security concern.
* If an attacker gains access, they couldescalate privileges and compromise the network.
* Investigatingunauthorized admin login attemptsshould be thetop priorityin a log audit.
* Why Other Options Are Incorrect:
* A (Endpoint not submitting logs):While this is concerning, it does not indicate anactive attack.
* B (Lateral movement):There's no evidence of a compromised account moving between servers yet.
* C (Misconfigured syslog server):False negatives are a possibility, but thefailed admin loginsare real.

NEW QUESTION # 528
.....

- TOP Free CAS-005 Practice - High-quality CompTIA CAS-005 Latest Test Materials: CompTIA SecurityX Certification Exam □ Enter [www.pdfvce.com] and search for ➽ CAS-005 □ to download for free □Reasonable CAS-005 Exam Price
- Reliable CAS-005 Test Duration □ Reliable CAS-005 Test Duration □ CAS-005 Pdf Version □ Search for ⇛ CAS-005 ⇚ and download it for free on ➤ www.dumpsmaterials.com □ website □Exam Dumps CAS-005 Provider
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ayurvedalibrary.net, gourabroy.com, myportal.utt.edu.tt, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Dumpcollection CAS-005 dumps now are free: https://drive.google.com/open?id=1uT-W6f0mHkDvSWo9OfNUu64Kv9_sMbw5