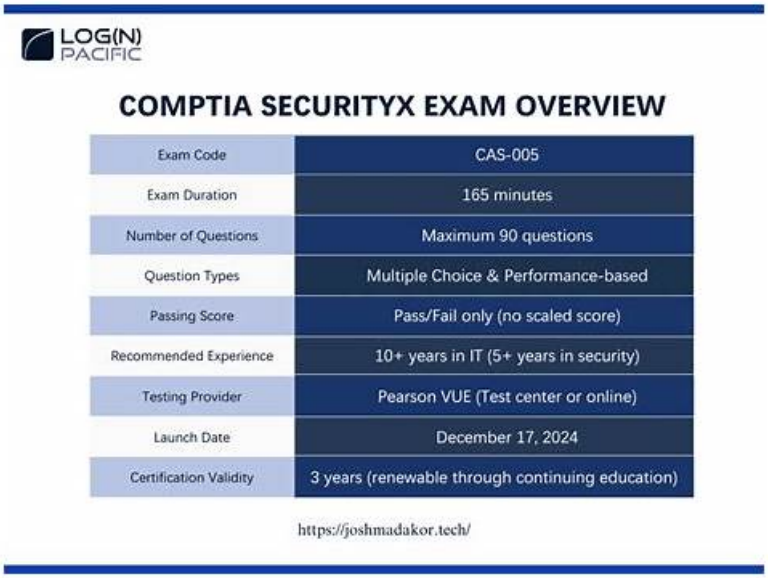
Pass for Sure CAS-005 Exam Cram Materials: CompTIA SecurityX Certification Exam are the best dumps for testers - ExamDumpsVCE



P.S. Free 2026 CompTIA CAS-005 dumps are available on Google Drive shared by ExamDumpsVCE: https://drive.google.com/open?id=18aZ7ac69MXYnR19AhSnXlxU3BKofpHnM

ExamDumpsVCE PDF questions can be printed. And this document of CAS-005 questions is also usable on smartphones, laptops and tablets. These features of the CompTIA SecurityX Certification Exam CAS-005 PDF format enable you to prepare for the test anywhere, anytime. By using the CAS-005 desktop practice exam software, you can sit in real exam like scenario. This CompTIA CAS-005 Practice Exam simulates the complete environment of the actual test so you can overcome your fear about appearing in the CompTIA SecurityX Certification Exam CAS-005 exam. ExamDumpsVCE has designed this software for your Windows laptops and computers.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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.

>> New CAS-005 Dumps Ppt <<

CompTIA CAS-005 Valid Exam Notes | Exam CAS-005 Outline

Our CompTIA Exam Questions greatly help CompTIA SecurityX Certification Exam (CAS-005) exam candidates in their preparation. Our CAS-005 practice questions are designed and verified by prominent and qualified CompTIA SecurityX Certification Exam (CAS-005) exam dumps preparation experts. The qualified CompTIA SecurityX Certification Exam (CAS-005) exam questions preparation experts strive hard and put all their expertise to ensure the top standard and relevancy of CAS-005 exam dumps topics.

CompTIA SecurityX Certification Exam Sample Questions (Q255-Q260):

NEW QUESTION # 255
A security engineer is reviewing the SIEM logs after a server crashed. The following list of events represents the timeline of actions collected from the SIEM:
Which of the following TTPs is most likely associated with this SIEM log?

- A. Lateral movement
- B. LOLBins use
- C. Data exfiltration
- D. Credential dumping

Answer: D

NEW QUESTION # 256
A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect
Which of the following security architect models is illustrated by the diagram?

- A. Perimeter protection security model
- B. Identity and access management model
- C. Zero Trust security model
- D. Agent based security model

Answer: C

Explanation:
The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is asecurity framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.
Key Characteristics of Zero Trust in the Diagram:
Role-based Access Control: Ensures that users have access only to the resources necessary for their role.
Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.
Network Access Control: Ensures that devices meet security standards before accessing the network.
Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.
This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.
Reference:
CompTIA SecurityX Study Guide
NIST Special Publication 800-207, "Zero Trust Architecture"
"Implementing a Zero Trust Architecture," Forrester Research

NEW QUESTION # 257
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent llS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:
Which of the following hosts should a security analyst patch first once a patch is available?

- A. 0
- B. 1

- C. 2
- D. 3
- E. 4
- F. 5

Answer: B

Explanation:
Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:
* Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
* Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
* Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies
* CIS Controls: Control 3 - Continuous Vulnerability Management

NEW QUESTION # 258
A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:
Which of the following is most likely the cause of the issue?

- A. The local network access has been configured tobypass MFA requirements.
- B. Several users have not configured their mobile devices toreceive OTP codes
- C. Administrator access from an alternate location is blocked by company policy
- D. A network geolocation is being misidentified by the authentication server

Answer: D

Explanation:
The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements.
The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.
Why Network Geolocation Misidentification?
Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.
Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.
Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.
Other options do not align with the pattern observed:
A). Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
C). Administrator access policy: This is about user access, not specific administrator access.
D). OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.
References:
CompTIA SecurityX Study Guide
"Geolocation and Authentication," NIST Special Publication 800-63B
"IP Geolocation Accuracy," Cisco Documentation

NEW QUESTION # 259
A security analystreviews the following report:
Which of the following assessments is the analyst performing?

- A. System
- B. Quantitative
- C. Supply chain
- D. Organizational

Answer: C

Explanation:
The table shows detailed information about products, includinglocation, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.
Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third- party components or insecure development practices.
Other types of assessments do not align with the detailed supplier and component information provided:
A). System: Focuses on individual system security, not the broader supply chain.
C). Quantitative: Focuses on numerical risk assessments, not supplier information.
D). Organizational: Focuses on internal organizational practices, not external suppliers.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
"Supply Chain Security Best Practices," Gartner Research

NEW QUESTION # 260
.....

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of ExamDumpsVCE CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=18aZ7ac69MXYnR19AhSnXlxU3BKofpHnM