Pass Guaranteed Quiz 2025 CompTIA CAS-005: CompTIA SecurityX Certification Exam First-grade Free Download

P.S. Free & New CAS-005 dumps are available on Google Drive shared by PassCollection: https://drive.google.com/open?id=1YLNRC6VQwRdtKr2cTUUZgARQ95oQiAu9

Our CAS-005 exam materials are compiled by experts and approved by the professionals who are experienced. They are revised and updated according to the pass exam papers and the popular trend in the industry. The language of our CAS-005 exam torrent is simple to be understood and our CAS-005 test questions are suitable for any learners. Only 20-30 hours are needed for you to learn and prepare our CAS-005 Test Questions for the exam and you will save your time and energy. No matter you are the students or the in-service staff you are busy in your school learning, your jobs or other important things and can't spare much time to learn.

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.

>> Free CAS-005 Download <<

New CAS-005 Test Preparation & Sample CAS-005 Exam

Our company has done the research of the CAS-005 study material for several years, and the experts and professors from our company have created the famous CAS-005 study materials for all customers. We believe our CAS-005 training braidump will meet all demand of all customers. If you long to pass the exam and get the certification successfully, you will not find the better choice than our CAS-005 Preparation questions. You can free dowload the demo of our CAS-005 exam questons to check the excellent quality on our website.

CompTIA SecurityX Certification Exam Sample Questions (Q290-Q295):

NEW QUESTION # 290
A company'sSIEMis designed to associate the company'sasset inventorywith user events. Given the following report:

Hostname	Account	Attempted Logins	Failed Logins	Successful Logins
Server 1	SalesUser	3	0	3
Server 2	AccountingUser	5	1	4
Server 3				
Server 4	Administrator	2	2	0
Server 4	HR.User	5	0	5
Server 5	Administrator	0	0	0

Which of thefollowing should asecurity engineer investigate firstas part of alog audit?

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

Answer: D

Explanation:
Comprehensive and Detailed
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 abrute-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 isCorrect:
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.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:SIEM & Incident Analysis MITRE ATT&CK (T1078.002):Valid Accounts - Administrator Compromise

NEW QUESTION # 291
During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities.
The code defects are causing product deployment delays. Which of the following is the best way to uncover these issues earlier in the life cycle?

- A. Directing application logs to the SIEM for continuous monitoring
- B. Modifying the WAF policies to block against known vulnerabilities
- C. Using a software dependency management solution

- D. Completing an IAST scan against the web application

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
SecurityX CAS-005 exam content emphasizes integrating security into the SDLC and using automated tools to identify vulnerabilities early.
* Software dependency management solutions track and analyze libraries and components for known vulnerabilities before deployment, using vulnerability databases such as NVD or OSS Index.
* IAST scanning still requires the application to be running and may detect issues later.
* WAF policies help block attacks in production but do not prevent vulnerable code from being deployed.
* SIEM monitoring is reactive and identifies issues after they occur.By detecting vulnerable dependencies early, software dependency management solutions prevent late-stage deployment delays and reduce security risk.

NEW QUESTION # 292
A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

- A. DORA
- B. CCPA
- C. GDPR
- D. COPPA

Answer: C

Explanation:
The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.
Reference:
CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.
GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.
"GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

NEW QUESTION # 293
A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

- A. Situational awareness
- B. Change management
- C. Compliance tracking
- D. Quality assurance

Answer: B

Explanation:
To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

NEW QUESTION # 294
An organization recently implemented a policy that requires all passwords to be rotated every 90 days. An administrator observes a

large volume of failed sign-on logs from multiple servers that are often accessed by users. The administrator determines users are disconnecting from the RDP session but not logging off. Which of the following should the administrator do to prevent account lockouts?

- A. Automate logout of inactive sessions.
- B. Extend the allowed session length.
- C. Enforce password complexity.
- D. Increase the account lockout threshold.

Answer: A

Explanation:
When users disconnect from Remote Desktop Protocol (RDP) sessions without properly logging off, their sessions remain active on the server. If their passwords are changed due to the 90-day rotation policy, these lingering sessions may attempt to reauthenticate using outdated credentials, leading to multiple failed login attempts and potential account lockouts.
Automating the logout of inactive sessions ensures that disconnected or idle sessions are terminated after a specified period, preventing stale sessions from causing authentication issues. This approach aligns with best practices for session management and helps maintain security compliance.
Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: "Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment."

NEW QUESTION # 295
.....