CAS-005 examkiller gültige Ausbildung Dumps & CAS-005 Prüfung Überprüfung Torrents

2026 Die neuesten ZertPruefung CAS-005 PDF-Versionen Prüfungsfragen und CAS-005 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1LErwjflYW2ybzXk0GVHFfG2BlKg_wxrH

Heute, wo das Internet schnell entwickelt, ist es ein übliches Phänomen, Online-Ausbildung zu wählen. ZertPruefung ist eine der vielen Online-Ausbildungswebsites. ZertPruefung hat langjährige Erfahrungen und kann den Kandidaten die Lernmaterialien von guter Qualität zur CompTIA CAS-005 Zertifizierungsprüfung bieten, um ihre Bedürfnisse abzudecken.

CompTIA CAS-005 Prüfungsplan:

Thema	Einzelheiten
Thema 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.
Thema 2	• 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.

Thema 3	• 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.
Thema 4	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

CAS-005 Deutsche - CAS-005 Zertifizierungsprüfung

Wenn Sie noch viel wertvolle Zeit und Energie für die Vorbereitung der CompTIA CAS-005 Zertifizierungsprüfung benutzen und nicht wissen, wie man mühlos und effizient die CompTIA CAS-005 Zertifizierungsprüfung bestehen kann, bieten jetzt ZertPruefung Ihnen eine effektive Methode, um die CompTIA CAS-005 Zertifizierungsprüfung zu bestehen. Mit ZertPruefung würden Sie bessere Resultate bei weniger Einsatz erzielen.

CompTIA SecurityX Certification Exam CAS-005 Prüfungsfragen mit Lösungen (Q297-Q302):

297. Frage
Users are experiencing a variety of issues when trying to access corporate resources examples include
* Connectivity issues between local computers and file servers within branch offices
* Inability to download corporate applications on mobile endpoints wtiilc working remotely
* Certificate errors when accessing internal web applications
Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

- A. Restore static content on lite CDN.
- B. Check IPS rules
- C. Implement advanced WAF rules.
- D. Validate MDM asset compliance
- E. Enable secure authentication using NAC
- F. Review VPN throughput

Antwort: D,F

Begründung:
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
A . Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
F . Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
B . Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.
C . Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
D . Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.
E . Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-77, "Guide to IPsec VPNs"
CIS Controls, "Control 11: Secure Configuration for Network Devices"

298. Frage
A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:
Which of the following is the most appropriate action for the analyst to take?

- A. Block employees from logging in to applications that are not part of their business area.
- B. implement automation to disable accounts that nave been associated with high-risk activity.
- C. Have the admin account owner change their password to avoid credential stuffing.
- D. Update the log configuration settings on the directory server that Is not being captured properly.

Antwort: B

Begründung:
The log-in activity indicates a security threat, particularly involving the ADMIN account with a high- risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

299. Frage
A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the most secure way to dispose of the SSDs given the CISO's concern?

- A. Overwriting
- B. Incinerating
- C. Formatting
- D. Degaussing
- E. Shredding

Antwort: B

Begründung:
For SSDs,incinerationis considered the most secure method of physical destruction, ensuring no data remanence. SSDs store data differently compared to traditional spinning disks, making degaussing ineffective. Overwriting and formatting may not reliably erase all storage cells due to wear-leveling technologies. Shredding may work if the granularity is extremely fine, but incineration guarantees complete destruction beyond recovery.
Reference:

300. Frage
After several companies in the financial industry were affected by a similar incident, they shared information about threat intelligence and the malware used for exploitation. Which of the following should the companies do to best indicate whether the attacks are being conducted by the same actor?

- A. Use IOC extractions.
- B. Look for common IOCs.
- C. Leverage malware detonation.
- D. Apply code stylometry.

Antwort: D

Begründung:
Determining if attacks are from the same actor requires unique attribution. Let's analyze:
A . Code stylometry:Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005's threat intelligence focus.
B . Common IOCs:Indicates similar attacks but not necessarily the same actor.
C . IOCextractions:Similar to B, lacks specificity for attribution.

301. Frage
Anorganization has noticed an increase in phishing campaigns utilizingtyposquatting. A security analyst needs to enrich the data for

commonly used domains against the domains used in phishing campaigns. The analyst uses a log forwarder to forward network logs to the SIEM. Which of the following would allow the security analyst to perform this analysis?

- A. Implement adashboardon the SIEM that shows the percentage of traffic by domain.
- B. Use acron jobto regularly update and compare domains.
- C. Create aparserthat matches domains.
- D. Develop aquerythat filters out all matching domain names.

Antwort: A

Begründung:
Enriching data to compare domains requires actionable visibility. Let's analyze:
A . Cron job:Automates updates but doesn't analyze in the SIEM.
B . Parser:Processes logs but doesn't provide comparison insights.
C . Filter query:Excludes matches, opposite of enrichment.

302. Frage
......