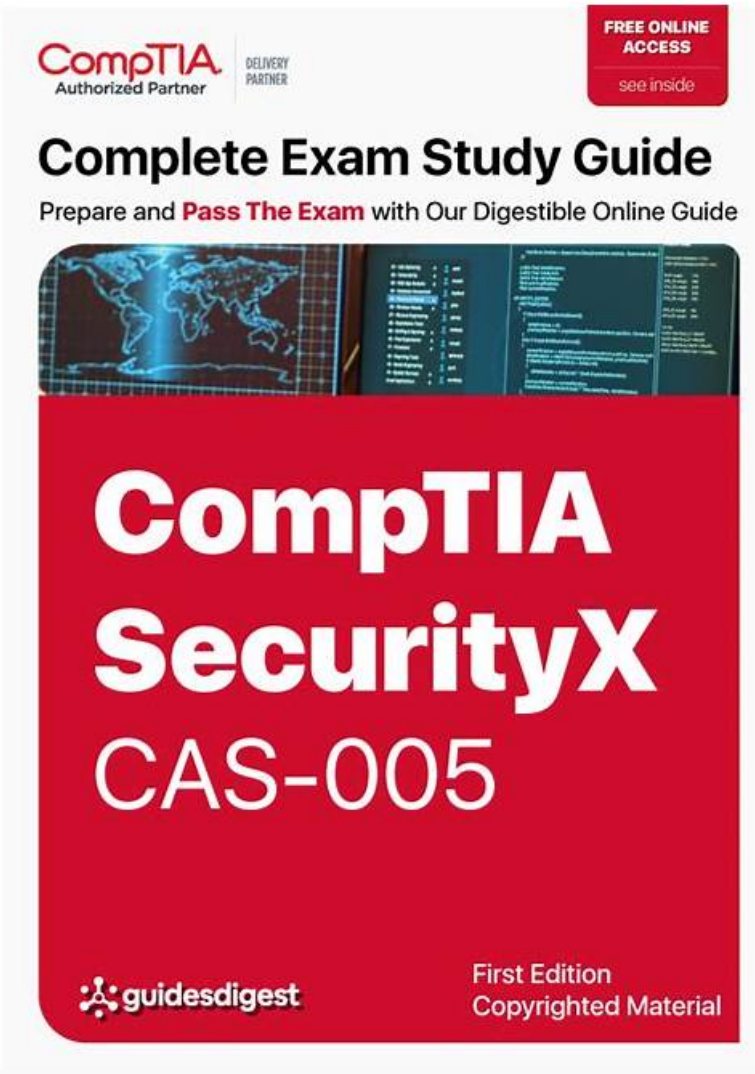
CAS-005 Testantworten & CAS-005 Prüfungsaufgaben



Die CompTIA CAS-005 Zertifizierungsprüfungen werden normalerweise von den IT-Spezialisten gemäß ihren Berufserfahrungen bearbeitet. So ist es auch bei PrüfungFrage. Die IT-Experten bieten Ihnen CompTIA CAS-005 Prüfungsfragen und Antworten (CompTIA SecurityX Certification Exam), mit deren Hilfe Sie die Prügung erfolgreich bestehen können. Die Genauigkeit von unseren Prüfungsfragen und Antworten beträgt 100%. Mit PrüfungFrage Produkten können Sie ganz leicht die CompTIA CAS-005 Zertifikate bekommen, was Ihnen eine große Beförderung in der IT-Branche ist.

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

Thema 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.
Thema 4	• 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.

CAS-005 Prüfungsaufgaben, CAS-005 Exam Fragen

Die Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung von PrüfungFrage sind die besten Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung. Sie sind die besten Schulungsunterlagen unter allen Schulungsunterlagen. Sie können Ihnen nicht nur helfen, die CompTIA CAS-005 Prüfung erfolgreich zu bestehen, Ihre Fachkenntnisse und Fertigkeiten zu verbessern und auch eine Karriere zu machen. Sie werden von allen Ländern gleich behandelt.

CompTIA SecurityX Certification Exam CAS-005 Prüfungsfragen mit Lösungen (Q32-Q37):

32. Frage
A company's help desk is experiencing a large number of calls from the finance department stating access issues to www bank com The security operations center reviewed the following security logs:

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User28	10.200.2.116/24	Finance	www.bank.com	65.146.76.34	495
User53	10.200.4.128/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

- A. The DNS record has been poisoned.
- B. The DNS was set up incorrectly.
- C. DNS traffic is being sinkholed.
- D. Recursive DNS resolution is failing

Antwort: C

Begründung:
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.
DNS poisoning (B) could result in usersbeing directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
References:
CompTIA SecurityX study materials on DNS security mechanisms.
Standard HTTP status codes and their implications.

33. Frage
A security analyst wants to use lessons learned from a prior incident response to reduce dwell time 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	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

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

Antwort: B

Begründung:
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.
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.

34. Frage
Which of the following best describes the reason a network architect would enable forward secrecy on all VPN tunnels?

- A. Modern cryptographic protocols list this process as a prerequisite for use.
- B. This process reduces the success of attackers performing cryptanalysis.
- C. This process is a requirement to enable hardware-accelerated cryptography.
- D. The business requirements state that confidentiality is a critical success factor.

Antwort: B

Begründung:
Forward secrecy, also known as perfect forward secrecy, is a feature of certain key agreement protocols that ensures session keys will not be compromised even if the server's private key is compromised in the future. By enabling forward secrecy on VPN tunnels, each session uses a unique key, and these keys are not derived from a common master key. This means that even if an attacker obtains the server's private key, they cannot decrypt past sessions, thereby significantly reducing the effectiveness of cryptanalysis attacks.

35. Frage
A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring. The architect's goal is to:
- Create a collection of use cases to help detect known threats
- Include those use cases in a centralized library for use across all
of the companies
Which of the following is the best way to achieve this goal?

- A. Sigma rules
- B. TAXII/STIX library
- C. UBA rules and use cases
- D. Ariel Query Language

Antwort: A

Begründung:
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option.
Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

36. Frage
A recent security audit identified multiple endpoints have the following vulnerabilities:
* Various unsecured open ports
* Active accounts for terminated personnel
* Endpoint protection software with legacy versions
* Overly permissive access rules
Which of the following would best mitigate these risks? (Select three).

- A. Local drive encryption
- B. Enabling BIOS password
- C. Unneeded services disabled
- D. Patching
- E. Address space layout randomization
- F. Logging
- G. Removal of unused accounts
- H. Secure boot

Antwort: C,D,G

Begründung:
Disabling unneeded servicesreduces the attack surface by closing open ports.Patchingensures that endpoint protection software and operating systems are up-to-date, reducing vulnerability exposure.Removing unused accountseliminates access paths for malicious users exploiting dormant accounts. Secure boot, BIOS passwords, and drive encryption are important, but they address different layers of security than the vulnerabilities listed.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply system hardening techniques to endpoint security issues.

37. Frage
.....

- CAS-005 Echte Fragen □ CAS-005 Prüfungen □ CAS-005 Zertifizierungsantworten □ Suchen Sie einfach auf [www.itzert.com] nach kostenloser Download von ✔ CAS-005 □✔□ □CAS-005 Prüfungen
- CAS-005 Demotesten □ CAS-005 Simulationsfragen □ CAS-005 Unterlage □ ▸ www.deutschpruefung.com ◂ ist die beste Webseite um den kostenlosen Download von □ CAS-005 □ zu erhalten □CAS-005 Prüfungen
- Aktuelle CompTIA CAS-005 Prüfung pdf Torrent für CAS-005 Examen Erfolg prep □ Suchen Sie auf ✔ www.itzert.com □✔□ nach ✔ CAS-005 □✔□ und erhalten Sie den kostenlosen Download mühelos □CAS-005 Probesfragen
- Die seit kurzem aktuellsten CompTIA CAS-005 Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der Prüfungen! □ Öffnen Sie die Webseite 《 www.deutschpruefung.com 》 und suchen Sie nach kostenloser Download von （ CAS-005 ） □CAS-005 Fragenkatalog
- CAS-005 Simulationsfragen □ CAS-005 Online Tests □ CAS-005 Zertifizierungsantworten □ Suchen Sie auf der Webseite ➽ www.itzert.com □ nach 《 CAS-005 》 und laden Sie es kostenlos herunter □CAS-005 Echte Fragen
- CAS-005 Der beste Partner bei Ihrer Vorbereitung der CompTIA SecurityX Certification Exam □ Öffnen Sie die Webseite ➽ www.pruefungfrage.de □ und suchen Sie nach kostenloser Download von ▹ CAS-005 ◃ □CAS-005 Simulationsfragen
- CAS-005 Prüfungen □ CAS-005 Prüfungs □ CAS-005 Deutsche □ Suchen Sie jetzt auf [www.itzert.com] nach □ CAS-005 □ um den kostenlosen Download zu erhalten □CAS-005 Deutsche
- CompTIA CAS-005: CompTIA SecurityX Certification Exam braindumps PDF - Testking echter Test □ Sie müssen nur zu 【 de.fast2test.com 】 gehen um nach kostenloser Download von □ CAS-005 □ zu suchen □CAS-005 Deutsch Prüfung
- CAS-005 Prüfungsfragen Prüfungsvorbereitungen, CAS-005 Fragen und Antworten, CompTIA SecurityX Certification Exam □ Suchen Sie jetzt auf 「 www.itzert.com 」 nach ➠ CAS-005 □ und laden Sie es kostenlos herunter □CAS-005 Zertifizierungsantworten
- CAS-005 Probesfragen □ CAS-005 Deutsche Prüfungsfragen □ CAS-005 Echte Fragen □ Suchen Sie auf ➽ www.pass4test.de □ nach ➤ CAS-005 □ und erhalten Sie den kostenlosen Download mühelos □CAS-005 Unterlage
- www.stes.tyc.edu.tw, esg.fit4dev.eu, zeeboomba.net, 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.vrdianpai.cn, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, educatorsempowerment.com, 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, Disposable vapes