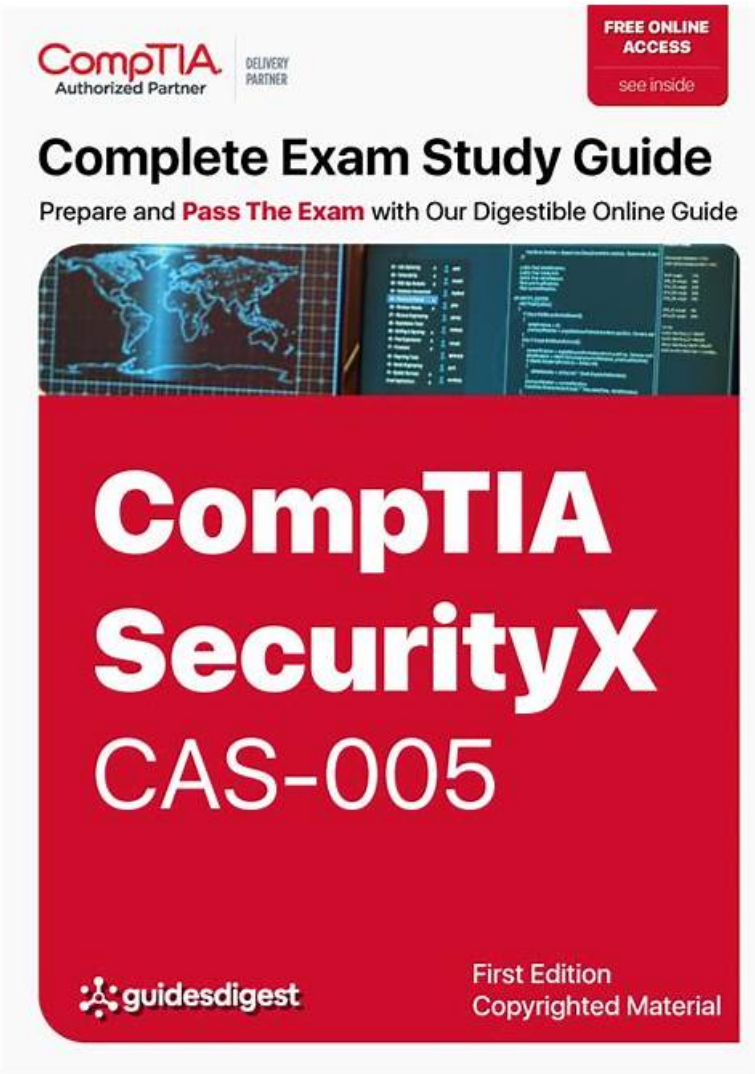
CAS-005 Zertifizierung, CAS-005 Prüfungen



Übrigens, Sie können die vollständige Version der ExamFragen CAS-005 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1xbb86wv6g5SYzpFC0Xr42zwfX1Sa_ean

Es ist besser, zu handeln als die anderen zu beneiden. Die Prüfungsmaterialien zur CompTIA CAS-005 Zertifizierungsprüfung von ExamFragen wird Ihr erster Schritt zum Erfolg. Mit ExamFragen können Sie sicher die schwierige CompTIA CAS-005 Prüfung bestehen. Mit diesem CompTIA CAS-005 Zertifikat können Sie ein Licht in Ihrem Herzen anzünden und neue Wege einschlagen und ein erfolgreiches Leben führen.

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 Zertifizierung <<

Valid CAS-005 exam materials offer you accurate preparation dumps

Als der professionelle Lieferant der IT-Zertifizierungsunterlagen, bieten wir ExamFragen immer die besten Unterlagen für Kandidaten und helfen vielen Leuten, die CompTIA CAS-005 Prüfung zu bestehen. Mit denen CompTIA CAS-005 Dumps von ExamFragen können Sie mehr selbstbewusster werden. Bei guter Nutzung der Dumps können Sie in sehr kürzer Zeit, die CompTIA CAS-005 Prüfung zu bestehen. Finden Sie es unglaublich? Aber es ist wirklich. Wenn Sie diese Unterlagensfragen von ExamFragen benutzen, können Sie das Wunder sehen.

CompTIA SecurityX Certification Exam CAS-005 Prüfungsfragen mit Lösungen (Q168-Q173):

168. Frage
During a security assessment, a penetration tester executed the following attack:

```
C:\> copy /y "C:\payloads\evil.exe" "C:\Program Files\Data Process\data.exe"
C:\Program Files\Data Process\> sc start data.exe
```

The tester then shared the results with the security analyst. Which of the following should the analyst do to remediate the attack?

- A. Enable user control access on the endpoint.
- B. Enable a PowerShell execution policy on the endpoint.
- C. Implement a security endpoint solution.
- D. Disable services with unquoted paths on the endpoint.

Antwort: D

169. Frage
A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code issaved lo the repository The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

- A. Pipeline compliance scanning
- B. Automated regression testing
- C. Pre-commit code linting
- D. Repository branch protection
- E. Code submit authorization workflow
- F. Software composition analysis

Antwort: B,C

Begründung:
B: Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.
D: Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into

the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.
Other options:
A: Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.
C: Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.
E: Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.
F: Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.

170. Frage
A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository The security team needs to be able to quickly evaluate whether to respond to a given vulnerability Which of the following, will allow the security team to achieve the objective with the last effort?

- A. SAST scan reports
- B. CIS benchmark compliance reports
- C. Credentialed vulnerability scan
- D. Centralized SBoM

Antwort: D

Begründung:
A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.
Why Centralized SBoM?
* Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
* Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
* Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.
* Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.
Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
* A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
* C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
* D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.
References:
* CompTIA SecurityX Study Guide
* "Software Bill of Materials (SBoM)," NIST Documentation
* "Managing Container Security with SBoM," OWASP

171. Frage
A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

Date & Time	Public IP	Browser Info	Action
11 Dec 22:30:23	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:05:43	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:10:29	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin
11 Dec 23:12:18	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Logoff
12 Dec 00:05:43	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin

Which of the following actions should the analyst take to best mitigate the threat?

- A. Implement WAF protection for the web application.

- B. Only allowconnections from approved IPs.
- C. Block IP 104.18.16.29 on the firewall.
- D. Upgrade the firmware on the camera.

Antwort: B

Begründung:
The logs indicate unauthorized access from104.18.16.29, an external IP, to the building camera's administrative console during off-hours.Restricting access only to approved IPsensures that only authorized personnel can remotely control the cameras, reducing the risk of unauthorized access and manipulation.
* Implementing WAF protection (A)secures against web application attacks but does not restrict unauthorized administrative access.
* Upgrading the firmware (B)is good security hygiene but does not immediately mitigate the active threat.
* Blocking IP 104.18.16.29 (D)is a temporary measure, as an attacker can switch to another IP. A better long-term solution is whitelisting trusted IPs.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section onAccess Control and Network Security

172. Frage
A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites
The server accepted the following 3 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA                56
TLS_RSA_WITH_AES_128_CBC_SHA            128
TLS_RSA_WITH_3DES_EDE_CBC_SHA           168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA       168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

- A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- B. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
- C. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
- D. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA
- E. Removing support for CBC-based key exchange and signing algorithms
- F. Implementing HIPS rules to identify and block BEAST attack attempts

Antwort: B,E

Begründung:
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
B . Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
C . Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"
OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

173. Frage
.....

- CAS-005 Schulungsangebot, CAS-005 Testing Engine, CompTIA SecurityX Certification Exam Trainingsunterlagen □ URL kopieren ➤ www.itzert.com □ Öffnen und suchen Sie 【 CAS-005 】 Kostenloser Download □CAS-005 Deutsche Prüfungsfragen
- CAS-005 Schulungsangebot, CAS-005 Testing Engine, CompTIA SecurityX Certification Exam Trainingsunterlagen □ Geben Sie ➽ www.itzert.com □ ein und suchen Sie nach kostenloser Download von ➥ CAS-005 □ □CAS-005 Pruefungssimulationen
- Die seit kurzem aktuellsten CompTIA SecurityX Certification Exam Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der CompTIA CAS-005 Prüfungen! □ Geben Sie ☀ www.zertpruefung.ch □☀□ ein und suchen Sie nach kostenloser Download von ➠ CAS-005 □ □CAS-005 Online Tests
- CAS-005 Studienmaterialien: CompTIA SecurityX Certification Exam - CAS-005 Zertifizierungstraining ◂ Öffnen Sie ▸ www.itzert.com ◂ geben Sie 《 CAS-005 》 ein und erhalten Sie den kostenlosen Download □CAS-005 Tests
- CAS-005 Tests □ CAS-005 Fragen&Antworten □ CAS-005 Deutsch Prüfungsfragen □ Suchen Sie jetzt auf ✔ www.pruefungfrage.de □✔□ nach ✔ CAS-005 □✔□ um den kostenlosen Download zu erhalten □CAS-005 Deutsch
- CAS-005 Online Tests □ CAS-005 Lernhilfe □ CAS-005 Dumps Deutsch □ Erhalten Sie den kostenlosen Download von ✔ CAS-005 □✔□ mühelos über 「 www.itzert.com 」 □CAS-005 Online Tests
- CAS-005 Schulungsangebot, CAS-005 Testing Engine, CompTIA SecurityX Certification Exam Trainingsunterlagen □ Öffnen Sie ▸ www.zertpruefung.ch ◂ geben Sie ➽ CAS-005 □ ein und erhalten Sie den kostenlosen Download □CAS-005 Dumps Deutsch
- CAS-005 Kostenlos Downloden □ CAS-005 Lernhilfe □ CAS-005 Online Tests □ Sie müssen nur zu □ www.itzert.com □ gehen um nach kostenloser Download von ➠ CAS-005 □ zu suchen □CAS-005 Ausbildungsressourcen
- CAS-005 Dumps Deutsch □ CAS-005 PDF Demo □ CAS-005 Zertifizierungsantworten □ Suchen Sie einfach auf ➠ de.fast2test.com □ nach kostenloser Download von { CAS-005 } □CAS-005 Deutsche Prüfungsfragen
- CAS-005 Lerntipps □ CAS-005 Lernhilfe □ CAS-005 Fragen Und Antworten □ Öffnen Sie die Website ➤ www.itzert.com □ Suchen Sie ▹ CAS-005 ◃ Kostenloser Download □CAS-005 Dumps
- CAS-005 Fragen&Antworten □ CAS-005 Lernressourcen □ CAS-005 Fragen Und Antworten □ Öffnen Sie die Webseite 《 www.zertpruefung.ch 》 und suchen Sie nach kostenloser Download von （ CAS-005 ） □CAS-005 Kostenlos Downloden
- www.freecram.com, arcoasiscareacademy.com, www.quora.com, lms.anatoliaec.com, www.stes.tyc.edu.tw, 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, 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, lms.ait.edu.za, 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

BONUS!!! Laden Sie die vollständige Version der ExamFragen CAS-005 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1xbb86wv6g5SYzpFC0Xr42zwfX1Sa_ean