

Quiz CompTIA - CAS-004 - Professional Valid CompTIA Advanced Security Practitioner (CASP+) Exam Exam Review

CompTIA CASP+ CAS-004

645 Practice Test Questions

in PDF Format with Verified Answers

P.S. Free & New CAS-004 dumps are available on Google Drive shared by Actual4Cert: <https://drive.google.com/open?id=1BoLYkyxONqzHhmGpQnxCNZsiH3EwV6ja>

In today's competitive industry, only the brightest and most qualified candidates are hired for high-paying positions. Obtaining CAS-004 is a wonderful approach to be successful because it can draw in prospects and convince companies that you are the finest in your field. Pass the CAS-004 Exam to establish your expertise in your field and receive certification. However, passing the CompTIA Advanced Security Practitioner (CASP+) Exam CAS-004 exam is challenging.

CompTIA CAS-004 certification exam covers a range of cybersecurity topics, including enterprise security architecture, risk management, incident response, research and analysis, and integration of computing, communications, and business disciplines. CompTIA Advanced Security Practitioner (CASP+) Exam certification exam also covers emerging technologies such as cloud computing, mobile devices, and virtualization.

CompTIA CAS-004 Exam covers a wide range of topics related to cybersecurity, including risk management, enterprise security architecture, research and collaboration, and integration of computing, communications, and business disciplines. CAS-004 exam also tests the candidate's knowledge of advanced security concepts such as cryptography, identity and access management, and secure communication protocols.

>> Valid CAS-004 Exam Review <<

Sample CompTIA CAS-004 Questions & CAS-004 Latest Practice Materials

First and foremost, we have high class operation system so we can assure you that you can start to prepare for the CAS-004 exam with our study materials only 5 to 10 minutes after payment. Fortunately, you need not to worry about this sort of question any more, since you can find the best solution in this website--our CAS-004 Training Materials. With our continued investment in technology, people and facilities, the future of our company has never looked so bright. There are so many advantages of our CAS-004 practice test and I would like to give you a brief introduction now.

CompTIA CAS-004 is an advanced level certification exam that validates the skills and knowledge of IT professionals in cybersecurity. CAS-004 exam is designed for those who are seeking to advance their careers in the field of cybersecurity by demonstrating their ability to configure and implement security solutions that protect against various cyber threats. CAS-004 Exam is intended for security professionals with at least 5 years of experience in the field.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q360-Q365):

NEW QUESTION # 360

An analyst determined that the current process for manually handling phishing attacks within the company is ineffective. The analyst is developing a new process to ensure phishing attempts are handled internally in an appropriate and timely manner. One of the analyst's requirements is that a blocklist be updated automatically when phishing attempts are identified. Which of the following would help satisfy this requirement?

- A. SOAR
- B. MSSP
- C. Virtualization
- D. MDR deployment
- E. Containerization

Answer: A

Explanation:

To automate the process of handling phishing attempts and updating blocklists, the best solution is to implement SOAR (Security Orchestration, Automation, and Response). SOAR platforms allow organizations to define automated workflows for responding to security incidents, such as phishing attacks. In this case, SOAR can automate the identification of phishing attempts and update blocklists in real-time, improving response time and consistency. MSSP (Managed Security Service Provider) and MDR (Managed Detection and Response) are outsourced services that do not directly address the need for automation, and containerization and virtualization are unrelated to incident handling.

NEW QUESTION # 361

An organization has just been breached, and the attacker is exfiltrating data from workstations.

The security analyst validates this information with the firewall logs and must stop the activity immediately. Which of the following steps should the security analyst perform NEXT?

- A. Determine where the data is being transmitted and create a block rule.
- B. Determine if a user inadvertently installed malware from a USB drive and update antivirus definitions.
- C. Determine which users may have clicked on a malicious email link and suspend their accounts.
- D. Determine if users have been notified to save their work and turn off their workstations.
- E. Determine what data is being stolen and change the folder permissions to read only.

Answer: A

NEW QUESTION # 362

The principal security analyst for a global manufacturer is investigating a security incident related to abnormal behavior in the ICS network. A controller was restarted as part of the troubleshooting process, and the following issue was identified when the controller was restarted:



SECURE BOOT FAILED: Firmware Mismatch Expected 0xFDC479 Actual 0x79F31B

During the investigation, this modified firmware version was identified on several other controllers at the site.

The official vendor firmware versions do not have this checksum. Which of the following stages of the MITRE ATT&CK framework for ICS includes this technique?

- A. Collection
- B. Lateral movement
- C. Evasion
- D. Persistence

Answer: D

Explanation:

The MITRE ATT&CK framework for ICS (Industrial Control Systems) details various tactics and techniques that may be used by adversaries. In the scenario described, the presence of unexpected firmware versions with a checksum that does not match the official vendor firmware indicates that the firmware has been modified. In the MITRE ATT&CK framework for ICS, this falls under the "Persistence" tactic, as it demonstrates an adversary's ability to maintain their foothold within the environment through unauthorized modification of device firmware.

NEW QUESTION # 363

An organization based in the United States is planning to expand its operations into the European market later in the year. Legal counsel is exploring the additional requirements that must be established as a result of the expansion. The BEST course of action would be to

- A. complete a quantitative risk assessment
- **B. complete a security questionnaire focused on data privacy.**
- C. revise the employee provisioning and deprovisioning procedures
- D. draft a memorandum of understanding

Answer: B

NEW QUESTION # 364

The IT team suggests the company would save money by using self-signed certificates, but the security team indicates the company must use digitally signed third-party certificates. Which of the following is a valid reason to pursue the security team's recommendation?

- **A. Private-key CSR signage prevents on-path interception.**
- B. PKCS #10 is still preferred over PKCS #12.
- C. There is minimal benefit in using a certificate revocation list.
- D. There is more control in using a local certificate over a third-party certificate.

Answer: A

Explanation:

Digitally signed third-party certificates provide greater security assurance because they are verified by trusted Certificate Authorities (CAs) and offer protection against on-path (man-in-the-middle) interception. Private-key Certificate Signing Request (CSR) signage helps ensure that communication cannot be intercepted or modified by malicious actors. Self-signed certificates, on the other hand, are not trusted outside the local environment and do not provide the same level of protection against on-path attacks. CASP+ emphasizes the security benefits of using third-party-signed certificates for securing communications over public networks.

Reference:

CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (PKI, SSL/TLS Certificates) CompTIA

CASP+ Study Guide: The Role of Certificate Authorities in Secure Communication

NEW QUESTION # 365

.....

Sample CAS-004 Questions: <https://www.actual4cert.com/CAS-004-real-questions.html>

- CAS-004 Minimum Pass Score ☐ CAS-004 Exam Actual Tests ☐ CAS-004 Reliable Test Book ☐ The page for free download of "CAS-004" on ☐ www.pass4test.com ☐ will open immediately ☐ Authorized CAS-004 Pdf
- Updated Valid CAS-004 Exam Review Help You to Get Acquainted with Real CAS-004 Exam Simulation ☐ Simply search for ➡ CAS-004 ☐☐☐ for free download on ☐ www.pdfvce.com ☐ ☐ Valid CAS-004 Test Book
- CAS-004 Exam Actual Tests ☐ Valid CAS-004 Test Notes ☐ Free CAS-004 Dumps ☐ Open ➡ www.testsimulate.com ☐ enter ➡ CAS-004 ☐☐☐ and obtain a free download ☐ CAS-004 Minimum Pass Score
- 100% Free CAS-004 – 100% Free Valid Exam Review | Excellent Sample CompTIA Advanced Security Practitioner (CASP+) Exam Questions ☐ Easily obtain ✓ CAS-004 ☐ ✓ ☐ for free download through ➤ www.pdfvce.com ☐ ☐ Valid CAS-004 Test Notes
- CAS-004 Valid Braindumps Questions ☐ Free CAS-004 Dumps ☐ Valid CAS-004 Test Notes ☐ Download ➤

CAS-004 ☐ for free by simply searching on “ www.prep4away.com ” ☐Authorized CAS-004 Pdf

- 2025 The Best Valid CAS-004 Exam Review | 100% Free Sample CompTIA Advanced Security Practitioner (CASP+) Exam Questions ☐ Download ⇒ CAS-004 ⇐ for free by simply searching on [www.pdfvce.com] ☐CAS-004 Latest Braindumps
- Reliable CAS-004 Test Question ☐ Valid CAS-004 Test Book ☐ Valid CAS-004 Test Book ☐ Enter ☐ www.torrentvalid.com ☐ and search for ▷ CAS-004 ◁ to download for free ☐Valid CAS-004 Test Notes
- Updated Valid CAS-004 Exam Review Help You to Get Acquainted with Real CAS-004 Exam Simulation ☐ Open 「 www.pdfvce.com 」 enter ☐ CAS-004 ☐ and obtain a free download ☐Valid CAS-004 Test Notes
- CAS-004 Latest Exam Papers ☐ CAS-004 Exam Actual Tests ☐ New CAS-004 Study Guide ☐ Easily obtain free download of ➡ CAS-004 ☐ by searching on { www.pdfdumps.com } ☐CAS-004 Knowledge Points
- Valid CAS-004 Exam Review - Pass Guaranteed 2025 CompTIA CAS-004 First-grade Sample Questions ☐ Copy URL 【 www.pdfvce.com 】 open and search for 【 CAS-004 】 to download for free ☐Valid CAS-004 Test Book
- CAS-004 Knowledge Points ☐ CAS-004 Minimum Pass Score ☐ CAS-004 Testing Center ☐ Open ⇒ www.testsdumps.com ⇐ and search for ➡ CAS-004 ☐☐☐ to download exam materials for free ☐Reliable CAS-004 Test Question
- johnlee994.webbuzzfeed.com, www.stes.tyc.edu.tw, huntertraders.com, study.stcs.edu.np, 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, www.stes.tyc.edu.tw, www.zylt.org, daotao.wisebusiness.edu.vn, quokkademy.com, 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!!! Download part of Actual4Cert CAS-004 dumps for free: [https://drive.google.com/open?](https://drive.google.com/open?id=1BoLYkyxONqzHhmGpQnxCNZsiH3EwV6ja)

[id=1BoLYkyxONqzHhmGpQnxCNZsiH3EwV6ja](https://drive.google.com/open?id=1BoLYkyxONqzHhmGpQnxCNZsiH3EwV6ja)