

Pdf Demo CAS-004 Download & CAS-004 Reliable Test Camp



P.S. Free & New CAS-004 dumps are available on Google Drive shared by BraindumpsIT: https://drive.google.com/open?id=1Wjo44F7FO02fZd01Bry_-ujPInC8ke6p

Choose BraindumpsIT CAS-004 new dumps questions, you will never regret for your decision. Our high-quality CAS-004 exam cram can ensure you 100% pass. You see, we have quality control system, each questions of CAS-004 exam dumps are checked and confirmed strictly according to the quality control system. Besides, the updated frequency for CAS-004 Exam Questions is so regular and in accordance with the real exam changes. You can enjoy one year free update after purchase.

Our CAS-004 exam questions own a lot of advantages that you can't imagine. First of all, all content of our CAS-004 study guide is accessible and easy to remember, so no need to spend a colossal time to practice on it. Second, our CAS-004 training quiz is efficient, so you do not need to disassociate yourself from daily schedule. Just practice with our CAS-004 learning materials on a regular basis and everything will be fine.

>> **Pdf Demo CAS-004 Download <<**

CAS-004 Reliable Test Camp | CAS-004 Reliable Braindumps

Many clients may worry that their privacy information will be disclosed while purchasing our CAS-004 quiz torrent. We promise to you that our system has set vigorous privacy information protection procedures and measures and we won't sell your privacy information. Before you buy our product, you can download and try out it freely so you can have a good understanding of our CAS-004 Quiz prep. Please feel safe to purchase our CAS-004 exam torrent any time as you like. We provide the best service to the client and hope the client can be satisfied.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q163-Q168):

NEW QUESTION # 163

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk,

but the developers cannot fix the issue right away.

Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

- A. Change privileged usernames, review the OS logs, and deploy hardware tokens.
- B. **Implement MFA, review the application logs, and deploy a WAF.**
- C. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
- D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: B

Explanation:

Reference: <https://www.microfocus.com/en-us/what-is/sast>

Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited.

Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability.

While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

NEW QUESTION # 164

A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

- A. **Mitigate**
- B. Avoid
- C. Transfer
- D. Accept

Answer: A

NEW QUESTION # 165

A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst.

Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis.

A security engineer is concerned about the security of the solution and notes the following.

- * The critical device send cleartext logs to the aggregator.
- * The log aggregator utilize full disk encryption.
- * The log aggregator sends to the analysis server via port 80.
- * MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.
- * The data is compressed and encrypted prior to being achieved in the cloud.

Which of the following should be the engineer's GREATEST concern?

- A. Multinancy and data remnants in the cloud
- B. Hardware vulnerabilities introduced by the log aggregate server
- C. **Encryption of data in transit**
- D. Network bridging from a remote access VPN

Answer: C

Explanation:

Explanation

Encryption of data in transit should be the engineer's greatest concern regarding the security of the solution.

Data in transit refers to data that is being transferred over a network or between devices. If data in transit is not encrypted, it can be intercepted, modified, or stolen by attackers who can exploit vulnerabilities in the network protocols or devices. The solution in the question sends logs from the critical devices to the aggregator in cleartext and from the aggregator to the analysis server via port 80, which are both insecure methods that expose the data to potential attacks. Verified References:

<https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://us-cert.cisa.gov/ncas/tips/ST04-019>

NEW QUESTION # 166

A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

- A. DLP
- B. UTM
- C. Data flow enforcement
- D. Mail gateway

Answer: A

NEW QUESTION # 167

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.

Which of the following will allow the inspection of the data without multiple certificate deployments?

- A. Include all available cipher suites.
- B. Implement certificate pinning.
- C. Create a wildcard certificate.
- D. Use a third-party CA.

Answer: C

Explanation:

A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates.

Using a third-party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate.

Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected certificate or public key in the application code, not a type of certificate. Verified References:

<https://www.comptia.org/blog/what-is-a-wildcard-certificate>

<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION # 168

.....

BraindumpsIT is a website to achieve dreams of many IT people. BraindumpsIT provide candidates participating in the IT certification exams the information they want to help them pass the exam. Do you still worry about passing CompTIA certification CAS-004 exam? Have you thought about purchasing an CompTIA certification CAS-004 exam counseling sessions to assist you? BraindumpsIT can provide you with this convenience. BraindumpsIT's training materials can help you pass the certification exam. BraindumpsIT's exercises are almost similar to real exams. With BraindumpsIT's accurate CompTIA Certification CAS-004 Exam practice questions and answers, you can pass CompTIA certification CAS-004 exam with a high score.

CAS-004 Reliable Test Camp: https://www.braindumpsit.com/CAS-004_real-exam.html

CompTIA Pdf Demo CAS-004 Download Moreover, if you fail the exam unfortunately, we give back you full refund or switch other versions freely, and it all up to you, CompTIA Pdf Demo CAS-004 Download In a matter of days, if not hours, our clients' purchases are updated with newly introduced questions within the offer of 90 days of free updates, CompTIA Pdf Demo CAS-004 Download And it is also what all of the candidates care about.

The following appendices are provided in this New CAS-004 Exam Cram book: A, I have no problem with disagreement and even strong dialogue, Moreover, if you fail the exam unfortunately, we Pdf Demo CAS-004 Download give back you full refund or switch

other versions freely, and it all up to you.

Pass Guaranteed 2026 CompTIA CAS-004: CompTIA Advanced Security Practitioner (CASP+) Exam Useful Pdf Demo Download

In a matter of days, if not hours, our clients' purchases are updated CAS-004 with newly introduced questions within the offer of 90 days of free updates. And it is also what all of the candidates care about.

And besides, you can take it with you wherever you go for it is portable and takes no place, Our staff will create a unique study plan for you based on the choice of the right version of the CAS-004 exam questions.

P.S. Free & New CAS-004 dumps are available on Google Drive shared by BraindumpsIT: https://drive.google.com/open?id=1Wjo44F7FO02fZd01Bry_-ujPInC8ke6p