CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.

B. Sign the key with DSA.

C. Deploy MFA for the service accounts.

D. Utilize HMAC for the keys.

Correct Answer: D

QUESTION 2

A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine\\'s operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider\\'s limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?

A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.

B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.

C. Implement a centralized network gateway to bridge network traffic between all VPCs.

D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Correct Answer: A

The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

QUESTION 3

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 aggregator and allows remote access to MSSP analysts. 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 aggregator to a public IP address in the MSSP\\'s datacenter for analysis. A security engineer is concerned about the secunty of the solution and notes the following

1.

The critical devices send cleartext logs to the aggregator.

2.

The log aggregator utilizes full disk encryption.

3.

The log aggregator sends to the analysis server via port 80.

4.

MSSP analysts utilize an SSL VPN with MFA to access the log aggregator remotely.

5.

The data is compressed and encrypted prior to being archived in the cloud.

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

A. Hardware vulnerabilities introduced by the log aggregator server.

B. Network bridging from a remote access VPN.

C. Encryption of data in transit.

D. Multitenancy and data remnants in the cloud.

Correct Answer: C

QUESTION 4

A forensic investigator started the process of gathering evidence on a laptop in response to an incident. The investigator took a snapshot of the hard drive, copied relevant log files, and then performed a memory dump. Which of the following steps in the process should have occurred FIRST?

A. Preserve secure storage.

B. Clone the disk.

C. Collect the most volatile data.

D. Copy the relevant log files.

Correct Answer: C

QUESTION 5

A developer needs to implement PKI in an autonomous vehicle\\'s software in the most efficient and labor-effective way possible. Which of the following will the developer MOST likely implement?

A. Certificate chain

B. Root CA

C. Certificate pinning

D. CRL

E. OCSP

Correct Answer: B

The developer would most likely implement a Root CA in the autonomous vehicle\\'s software. A Root CA is the top-level authority in a PKI that issues and validates certificates for subordinate CAs or end entities. A Root CA can be self-signed

and embedded in the vehicle\\'s software, which would reduce the need for external communication and verification. A Root CA would also enable the vehicle to use digital signatures and encryption for secure communication with other vehicles

or infrastructure. Verified References:

https://cse.iitkgp.ac.in/~abhij/publications/PKI++.pdf https://www.digicert.com/blog/connected-cars-need-security-use-pki https://ieeexplore.ieee.org/document/9822667/