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.pass4itsure.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

A security review of the architecture for an application migration was recently completed. The following observations were made:

1.

External inbound access is blocked.

2.

A large amount of storage is available.

3.

Memory and CPU usage are low.

4.

The load balancer has only a single server assigned.

5.

Multiple APIs are integrated.

Which of the following needs to be addressed?

A. Scalability

B. Automation

C. Availability

D. Performance

Correct Answer: A

The observation that the load balancer has only a single server assigned suggests an issue with scalability. Scalability refers to the ability of the system to handle increasing loads by adding resources. In this case, having a single server assigned to a load balancer may not be adequate to handle increased traffic or load, which could lead to performance issues.

QUESTION 2

A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. Which of the following would BEST prevent this scenario form happening again?

A. Performing routine tabletop exercises

B. Implementing scheduled, full interruption tests

C. Backing up system log reviews

D. Performing department disaster recovery walk-throughs

Correct Answer: B

QUESTION 3

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.

B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.

C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Correct Answer: C

QUESTION 4

A consultant needs access to a customer\\'s cloud environment. The customer wants to enforce the following engagement requirements:

1.

All customer data must remain under the control of the customer at all times.

2.

Third-party access to the customer environment must be controlled by the customer.

3.

Authentication credentials and access control must be under the customer\\'s control.

Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. Use the customer\\'s SSO with read-only credentials and share data using the customer\\'s provisioned secure network storage.

B. Use the customer-provided VDI solution to perform work on the customer\\'s environment.

C. Provide code snippets to the customer and have the customer run code and securely deliver its output.

D. Request API credentials from the customer and only use API calls to access the customer\\'s environment.

Correct Answer: B

Virtual Desktop Infrastructure (VDI) allows the consultant to work within a virtualized environment controlled by the customer. All data remains within the customer\\'s environment, and access is controlled by the customer.

QUESTION 5

A financial institution generates a list of newly created accounts and sensitive information on a daily basis. The financial institution then sends out a file containing thousands of lines of data. Which of the following would be the best way to reduce the risk of a malicious insider making changes to the file that could go undetected?

A. Write a SIEM rule that generates a critical alert when files are created on the application server.

B. Implement a FIM that automatically generates alerts when the file is accessed by IP addresses that are not associated with the application.

C. Create a script that compares the size of the file on an hourly basis and generates alerts when changes are identified.

D. Tune the rules on the host-based IDS for the application server to trigger automated alerts when the application server is accessed from the internet.

Correct Answer: B

File Integrity Monitoring (FIM) is a technology that can detect changes in files, often used to safeguard critical data. Implementing a FIM solution that generates alerts for access by unauthorized IP addresses would ensure that any unauthorized modifications to the file can be detected and acted upon. This helps in mitigating the risk of insider threats, as it would alert to any changes not made through the expected application process.

Latest CAS-004 Dumps CAS-004 Practice Test CAS-004 Exam Questions