# CAS-004<sup>Q&As</sup>

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**

The Chief Security Officer (CSO) requested the security team implement technical controls that meet the following requirements:

1.

Monitors traffic to and from both local NAS and cloud-based file repositories

2.

Prevents on-site staff who are accessing sensitive customer PII documents on file repositories from accidentally or deliberately sharing sensitive documents on personal SaaS solutions

3.

Uses document attributes to reduce false positives

4.

Is agentless and not installed on staff desktops or laptops

Which of the following when installed and configured would BEST meet the CSO\\'s requirements? (Choose two.)

A. DLP

B. NGFW

C. UTM

D. UEBA

E. CASB

F. HIPS

Correct Answer: AE

**QUESTION 2**

A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.

This is an example of:

A. due intelligence

B. e-discovery.

C. due care.

D. legal hold.

Correct Answer: B

## QUESTION 3

A security engineer needs to implement a CASB to secure employee user web traffic. A key requirement is that the relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to

expand traffic visibility. The solution must be highly resilient to network outages.

Which of the following architectural components would BEST meet these requirements?

A. Log collection

B. Reverse proxy

C. AWAF

D. API mode

Correct Answer: A

## QUESTION 4

A company would like to obfuscate PII data accessed by an application that is housed in a database to prevent unauthorized viewing. Which of the following should the company do to accomplish this goal?

A. Use cell-level encryption.

B. Mask the data.

C. Implement a DLP solution.

D. Utilize encryption at rest.

Correct Answer: B

## QUESTION 5

A security engineer has recently become aware of a Java application that processes critical information in real time on the company\\'s network. The Java application was scanned with SAST prior to deployment, and all vulnerabilities have been mitigated. However, some known issues within the Java runtime environment cannot be resolved. Which of the following should the security engineer recommend to the developer in order to mitigate the issue with the LEAST amount of downtime?

A. Perform software composition analysis on libraries from third parties.

B. Run the application in a sandbox and perform penetration tests.

C. Rewrite and compile the application in C++ and then reinstall it.

D. Embed the current application into a virtual machine that runs on dedicated hardware.

Correct Answer: D

By running the application in a dedicated virtual machine (VM), it\\'s isolated from the rest of the environment. This containment reduces the potential impact of vulnerabilities in the Java runtime since they\\'d be restricted to the VM. Moreover, embedding an application into a VM typically has a shorter downtime than rewriting the application or extensive testing.

Latest CAS-004 Dumps          CAS-004 Study Guide          CAS-004 Exam Questions