

CAS-003^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

<https://www.pass2lead.com/cas-003.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 manufacturing company employs SCADA systems to drive assembly lines across geographically dispersed sites. Therefore, the company must use the Internet to transport control messages and responses. Which of the following architectural changes when integrated will BEST reduce the manufacturing control system's attack surface? (Select TWO)

- A. Design a patch management capability for control systems.
- B. Implement supply chain security.
- C. Integrate message authentication
- D. Add sensors and collectors at the Internet boundary.
- E. Isolate control systems from enterprise systems.
- F. Implement a site-to-site VPN across sites

Correct Answer: AE

QUESTION 2

An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others.

Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

- A. Deploy virtual desktop infrastructure with an OOB management network
- B. Employ the use of vT PM with boot attestation
- C. Leverage separate physical hardware for sensitive services and data
- D. Use a community CSP with independently managed security services
- E. Deploy to a private cloud with hosted hypervisors on each physical machine

Correct Answer: AC

QUESTION 3

A company has experienced negative publicity associated with users giving out their credentials accidentally or sharing intellectual secrets were not properly defined. The company recently implemented some new policies and is now testing

their effectiveness. Over the last three months, the number of phishing victims dropped from 100 to only two in the last test. The DLP solution that was implemented catches potential material leaks, and the user responsible is retrained

Personal email accounts and USB drives are restricted from the corporate network.

Given the improvements, which of the following would a security engineer identify as being needed in a gap analysis?

- A. Additional corporate-wide training on phishing.
- B. A policy outlining what is and is not acceptable on social media.
- C. Notifications when a user falls victim to a phishing attack.
- D. Positive DLP preventions with stronger enforcement.

Correct Answer: B

QUESTION 4

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

- A. Synchronous copy of data
- B. RAID configuration
- C. Data de-duplication
- D. Storage pool space allocation
- E. Port scanning
- F. LUN masking/mapping
- G. Port mapping

Correct Answer: FG

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in `Zoning`. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

QUESTION 5

Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

- A. A spear-phishing email with a file attachment
- B. A DoS using IoT devices
- C. An evil twin wireless access point
- D. A domain hijacking of a bank website

Correct Answer: A

[CAS-003 PDF Dumps](#)

[CAS-003 Study Guide](#)

[CAS-003 Exam Questions](#)