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

When managing and mitigating SaaS cloud vendor risk, which of the following responsibilities belongs to the client?

A. Data

B. Storage

C. Physical security

D. Network

Correct Answer: A

QUESTION 2

A security engineer is re-architecting a network environment that provides regional electric distribution services. During a pretransition baseline assessment, the engineer identified the following security-relevant characteristics of the environment:

1.

Enterprise IT servers and supervisory industrial systems share the same subnet.

2.

Supervisory controllers use the 750MHz band to direct a portion of fielded PLCs.

3.

Command and telemetry messages from industrial control systems are unencrypted and unauthenticated.

Which of the following re-architecture approaches would be best to reduce the company\\'s risk?

A. Implement a one-way guard between enterprise IT services and mission-critical systems, obfuscate legitimate RF signals by broadcasting noise, and implement modern protocols to authenticate ICS messages.

B. Characterize safety-critical versus non-safety-critical systems, isolate safety-critical systems from other systems, and increase the directionality of RF links in the field.

C. Create a new network segment for enterprise IT servers, configure NGFW to enforce a well-defined segmentation policy, and implement a WIDS to monitor the spectrum.

D. Segment supervisory controllers from field PLCs, disconnect the entire network from the internet, and use only the 750MHz link for controlling energy distribution services.

Correct Answer: C

The best approach to reduce the company\\'s risk is to segregate the enterprise IT servers and supervisory industrial systems. Creating a new network segment and using a Next- Generation Firewall (NGFW) to enforce a strict segmentation policy will help to isolate the systems and protect against potential attacks. Additionally, implementing a Wireless Intrusion Detection System (WIDS) can help monitor the spectrum for unauthorized devices or interference.

QUESTION 3

An organization recently completed a security controls assessment. The results highlighted the following vulnerabilities:

1.

Out-of-date definitions

2.

Misconfigured operating systems

3.

An inability to detect active attacks

4.

Unimpeded access to critical servers' USB ports

Which of the following will most likely reduce the risks that were identified by the assessment team?

A. Install EDR on endpoints, configure group policy, lock server room doors, and install a camera system with guards watching 24/7.

B. Create an information security program that addresses user training, perform weekly audits of user workstations, and utilize a centralized configuration management program.

C. Update antivirus definitions, install NGFW with logging enabled, use USB port lockers, and run SCAP scans weekly.

D. Implement a vulnerability management program and a SIEM tool with alerting, install a badge system with zones, and restrict privileged access.

Correct Answer: C

QUESTION 4

A BIA of a popular online retailer identified several mission-essential functions that would take more than seven days to recover in the event of an outage. Which of the following should be considered when setting priorities for the restoration of these functions?

A. Supply chain issues

B. Revenue generation

C. Warm-site operations

D. Scheduled impacts to future projects

Correct Answer: B

QUESTION 5

A security administrator is confirming specific ports and IP addresses that are monitored by the IPS- IDS system as well as the firewall placement on the perimeter network between the company and a new business partner Which of the following business documents defines the parameters the security administrator must confirm?

A. BIA

B. ISA

C. NDA

D. MOU

Correct Answer: A