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

QUESTION 1

A host on a company\\'s network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.

Which of the following steps would be best to perform FIRST?

A. Turn off the infected host immediately.

B. Run a full anti-malware scan on the infected host.

C. Modify the smb.conf file of the host to prevent outgoing SMB connections.

D. Isolate the infected host from the network by removing all network connections.

Correct Answer: D

QUESTION 2

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company\\'s web store so they can resell it on the secondary market. The company\\'s intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems.

Which of the following now describes the level of risk?

A. Inherent

B. Low

C. Mitigated

D. Residual.

E. Transferred

Correct Answer: D

QUESTION 3

A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility

B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts

C. Implementing integrity checks on endpoint computing devices

D. Looking for privileged credential reuse on the network

Correct Answer: A

QUESTION 4

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage. Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency

B. Data exposure

C. Data loss

D. Data dispersion

Correct Answer: B

QUESTION 5

A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company\\'s CI/CD pipeline?

A. Utilizing a trusted secrets manager

B. Performing DAST on a weekly basis

C. Introducing the use of container orchestration

D. Deploying instance tagging

Correct Answer: A

Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/