CS0-003 $^{\text{Q\&As}}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

QUESTION 1

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

A. Human resources must email a copy of a user agreement to all new employees

B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement

C. All new employees must take a test about the company security policy during the cjitoardmg process

D. All new employees must sign a user agreement to acknowledge the company security policy

Correct Answer: D

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding " networks, or resources, as well as the consequences of violatin" Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

QUESTION 2

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication.

Which of the following does this most likely describe?

A. System hardening

B. Hybrid network architecture

C. Continuous authorization

D. Secure access service edge

Correct Answer: A

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system. The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

QUESTION 3

A security analyst needs to provide evidence of regular vulnerability scanning on the company\\'s network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

A. OpenVAS

B. Burp Suite

C. Nmap

D. Wireshark

Correct Answer: A

Explanation: OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

QUESTION 4

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators

B. Improve employee training and awareness

C. Increase password complexity standards

D. Deploy mobile device management

Correct Answer: B

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

QUESTION 5

Which of the following threat actors is most likely to target a company due to its questionable environmental policies?

A. Hacktivist

B. Organized crime

C. Nation-state

D. Lone wolf

Correct Answer: A

Explanation: Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets12. References: An introduction to the cyber threat environment, page 3; What is a Threat Actor? Types and Examples of Cyber Threat Actors, section 2.

Latest CS0-003 Dumps   CS0-003 Practice Test   CS0-003 Braindumps