CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cs0-003.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

The email system administrator for an organization configured DKIM signing for all email legitimately sent by the organization. Which of the following would most likely indicate an email is malicious if the company\\'s domain name is used as both the sender and the recipient?

A. The message fails a DMARC check

B. The sending IP address is the hosting provider

C. The signature does not meet corporate standards

D. The sender and reply address are different

Correct Answer: A

Reference: https://easydmarc.com/tools/dmarc-lookup

QUESTION 2

A large company wants to address frequent outages on critical systems with a secure configurations program. The Chief Information Security Officer (CISO) has asked the analysts to conduct research and make recommendations for a cost-effective solution with the least amount of disruption to the business. Which of the following would be the best way to achieve these goals?

A. Adopt the CIS security controls as a framework, apply configurations to all assets, and then notify asset owners of the change.

B. Coordinate with asset owners to assess the impact of the CIS critical security controls, perform testing, and then implement across the enterprise.

C. Recommend multiple security controls depending on business unit needs, and then apply configurations according to the organization\\'s risk tolerance.

D. Ask asset owners which configurations they would like, compile the responses, and then present all options to the CISO for approval to implement.

Correct Answer: B

QUESTION 3

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

A. Insider threat

B. Ransomware group

C. Nation-state

D. Organized crime

Correct Answer: C

QUESTION 4

The security analyst received the monthly vulnerability report. The following findings were included in the report:

1.

Five of the systems only required a reboot to finalize the patch application

2.

Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls

B. Due diligence

C. Maintenance windows

D. Passive discovery

Correct Answer: A

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

QUESTION 5

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

A. Geoblock the offending source country.

B. Block the IP range of the scans at the network firewall.

C. Perform a historical trend analysis and look for similar scanning activity.

D. Block the specific IP address of the scans at the network firewall.

Correct Answer: B

For the ones thinking that a whole country should get blocked, think about the CEO going on a vacation in that country. Being unable to reach the office or the web site would probably not fly well.