200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

QUESTION 1

What is vulnerability management?

A. A security practice focused on clarifying and narrowing intrusion points.

B. A security practice of performing actions rather than acknowledging the threats.

C. A process to identify and remediate existing weaknesses.

D. A process to recover from service interruptions and restore business-critical applications

Correct Answer: C

Reference: https://www.brinqa.com/vulnerability-management-primer-part-2-challenges/

Vulnerability management is the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities.[1] Vulnerability management is integral to computer security and network security, and must not be confused with Vulnerability assessment" source: https://en.wikipedia.org/wiki/Vulnerability_management

QUESTION 2

An engineer is working on a ticket for an incident from the incident management team. A week ago, an external web application was targeted by a DDoS attack. Server resources were exhausted and after two hours, it crashed. An engineer was able to identify the attacker and technique used. Three hours after the attack, the server was restored and the engineer recommended implementing mitigation by Blackhole filtering and transferred the incident ticket back to the IR team. According to NIST.SP800-61, at which phase of the incident response did the engineer finish work?

A. post-incident activity

B. preparation

C. detection and analysis

D. containment, eradication, and recovery

Correct Answer: D

QUESTION 3

Which artifact is used to uniquely identify a detected file?

A. file timestamp

B. file extension

C. file size

D. file hash

Correct Answer: D

QUESTION 4

What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated

B. Data is accessible and available to permitted individuals

C. Data is unaltered and its integrity is preserved

D. Data is secure and unreadable without decrypting it

Correct Answer: D

QUESTION 5

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege

B. need to know

C. integrity validation

D. due diligence

Correct Answer: A