200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.pass4itsure.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is a difference between signature-based and behavior-based detection?

A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.

B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.

C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.

D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

Correct Answer: B

Instead of searching for patterns linked to specific types of attacks, behavior- based IDS solutions monitor behaviors that may be linked to attacks, increasing the likelihood of identifying and mitigating a malicious action before the network is compromised. https://accedian.com/blog/what-is-the-difference-between-signature-based- and-behavior-based-ids/

QUESTION 2

What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.

B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.

C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools

D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

Correct Answer: D

Reference: https://insights.profitap.com/tap-vs-span

QUESTION 3

Which statement describes threat hunting?

A. It is an activity by an entity to deliberately bring down critical internal servers.

B. It includes any activity that might go after competitors and adversaries to infiltrate their systems.

C. It is a vulnerability assessment conducted by cyber professionals.

D. It is a prevention activity to detect signs of intrusion, compromise, data theft, abnormalities, or malicious activity.

Correct Answer: D

QUESTION 4

How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.

B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.

C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.

D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Correct Answer: B

QUESTION 5

What is a Shellshock vulnerability?

A. command injection

B. cross site scripting

C. heap overflow

D. SQL injection

Correct Answer: A