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 SIEM and SOAR?

A. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.

B. SIEM\\'s primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.

C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.

D. SOAR\\'s primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/products/security/what-is-a-security- platform.html siem is log managment soar is vulnerability managment that automat and response

QUESTION 2

An engineer discovered a breach, identified the threat\\'s entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

A. Recover from the threat.

B. Analyze the threat.

C. Identify lessons learned from the threat.

D. Reduce the probability of similar threats.

Correct Answer: A

Per: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION 3

DRAG DROP

Drag and drop the security concept on the left onto the example of that concept on the right.

Select and Place:

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Correct Answer:

	Threat
	Vulnerability
	Risk Assessment
	Exploit

QUESTION 4

Which type of data consists of connection level, application-specific records generated from network traffic?

A. transaction data

B. location data

C. statistical data

D. alert data

Correct Answer: A

QUESTION 5

Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis

B. preparation

C. eradication

D. containment

Correct Answer: A

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity

Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide