

KillTest

높은 품질, 더 나은 서비스



연습 문제

<https://www.killtest.kr>

1년간 무료 업데이트 제공

Exam : **300-220**

Title : Conducting Threat Hunting
and Defending using Cisco
Technologies for CyberOps

Version : DEMO

1.What is the primary goal of threat hunting?

- A. To reactively respond to security incidents
- B. To proactively search for signs of malicious activity
- C. To ignore potential threats until they become critical
- D. To rely solely on automated tools for threat detection

Answer: B

2.What does the term "threat intelligence" refer to in the context of threat hunting?

- A. Real-time monitoring of network traffic
- B. Data collected from previous security incidents
- C. Predictive analysis of potential cyber threats
- D. Information about current and emerging threats

Answer: D

3.In relation to threat hunting, what does the acronym IOC stand for?

- A. Independent Observation Criteria
- B. Indicators of Compromise
- C. Internal Operations Center
- D. Incident Of Concern

Answer: B

4.What role does correlation play in threat hunting?

- A. It ensures that all identified threats are immediately blocked
- B. It connects various data points to identify potential threats
- C. It blocks incoming traffic from suspicious IP addresses
- D. It monitors user activity but does not correlate it with any other data

Answer: B

5.Which of the following is NOT a common data source used in threat hunting?

- A. Network traffic logs
- B. Employee payroll information
- C. Endpoint security logs
- D. DNS logs

Answer: B