Vendor: Cisco

Exam Code: 300-220

Exam Name: Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Version: DEMO

QUESTION 1
Which of the following is a common data source used in threat hunting?

A. HR databases
B. Social media feeds
C. Security logs
D. Customer reviews

Answer: C

QUESTION 2
What is the role of machine learning in threat hunting techniques?

A. To replace human analysts in the threat hunting process
B. To automate the entire threat detection process
C. To provide intelligence and analytics for detecting threats
D. To slow down the threat detection process

Answer: C

QUESTION 3
Which of the following techniques involves searching for indicators of compromise (IoC) in an organization's network?

A. NetFlow analysis
B. Geolocation tracking
C. Hashing algorithms
D. IoC scanning

Answer: D

QUESTION 4
What does the term "honeypot" refer to in threat hunting techniques?

A. A sweet treat for security analysts
B. A decoy system designed to lure attackers
C. A type of encryption algorithm
D. A tool used for network mapping

Answer: B

QUESTION 5
Which of the following is a common method for detecting phishing attacks in threat hunting techniques?

A. DNS monitoring
B. Predictive analytics
C. Asset management
D. Hardware encryption

Answer: A

QUESTION 6
What is the purpose of conducting penetration testing as part of threat hunting techniques?

A. To analyze financial data
B. To penetrate an organization's defenses
C. To simulate real-world attacks and identify vulnerabilities
D. To monitor employee behavior

Answer: C

QUESTION 7
Which of the following is an example of an active threat hunting technique?

A. Conducting regular vulnerability scans
B. Reviewing security logs after an incident
C. Monitoring network traffic in real-time
D. Waiting for alerts from automated security tools

Answer: C

QUESTION 8
Why is it important to document and communicate findings during the threat hunting process?

A. To keep sensitive information confidential
B. To ensure that all findings are thoroughly investigated
C. To maintain compliance with industry regulations
D. To share knowledge and improve overall security posture

Answer: D

QUESTION 9
What is the main focus of signature-based threat hunting techniques?

A. Identifying new, unknown threats
B. Matching known patterns and indicators of compromise
C. Utilizing machine learning algorithms for threat detection
D. Analyzing network traffic anomalies

Answer: B

QUESTION 10
What is the first step in the threat hunting process?

A. Analyzing log files
B. Identifying potential threats

C. Initiating incident response procedures
D. Developing threat models

Answer: B

QUESTION 11
During which phase of the threat hunting process are threat indicators analyzed and correlated?

A. Collection
B. Analysis
C. Investigation
D. Remediation

Answer: B

QUESTION 12
Which step in the threat hunting process involves examining network traffic patterns to identify anomalies?

A. Data Collection
B. Log Analysis
C. Network Traffic Analysis
D. Threat Correlation

Answer: C

QUESTION 13
In the context of the threat hunting process, what does the term "pivot" mean?

A. To move quickly from one hypothesis to another
B. To backtrack and analyze previous data
C. To rotate data points in a visualization
D. To confirm a suspected threat

Answer: A

QUESTION 14
Which phase of the threat hunting process involves analyzing security logs, network traffic, and endpoint data?

A. Data Collection
B. Data Processing
C. Data Analysis
D. Data Visualization

Answer: C

QUESTION 15

During the investigation phase of the threat hunting process, what activity is typically conducted?

A. Refining hypotheses
B. Collecting additional data
C. Generating threat intelligence reports
D. Mitigating the threat

Answer: A

QUESTION 16
Which step in the threat hunting process involves creating and executing queries to search for indicators of compromise?

A. Data Collection
B. Data Analysis
C. Data Processing
D. Data Enrichment

Answer: B

QUESTION 17
What is the final step in the threat hunting process?

A. Remediation
B. Reporting
C. Analysis
D. Attribution

Answer: B

QUESTION 18
What is the purpose of the data processing phase in the threat hunting process?

A. To prioritize threats based on severity
B. To enrich collected data with threat intelligence
C. To filter and normalize data for analysis
D. To block malicious traffic at the perimeter

Answer: C