Cisco.300-220.v2026-05-27.q60

Exam Code:	300-220
Exam Name:	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps
Certification Provider:	Cisco
Free Question Number:	60
Version:	v2026-05-27
# of views:	102
# of Questions views:	629
https://www.freecram.net/torrent/Cisco.300-220.v2026-05-27.q60.html	

NEW QUESTION: 1
The integration of which products would most enhance analytical capabilities for threat hunting?
A. Uncoordinated firewall and intrusion prevention systems
B. SIEM, EDR, and threat intelligence platforms
C. Standalone antivirus solutions
D. Disconnected SIEM and endpoint detection and response (EDR) platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 2
When determining the priority of attacks based on the Cyber Kill Chain, which stage is crucial for early detection?
A. Command and Control
B. Installation
C. Reconnaissance
D. Weaponization
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Attack remediation strategies should be based on:
A. The most expensive solution available
B. The latest tech trends
C. The results of a threat assessment
D. The personal preferences of the security team
Answer: (SHOW ANSWER)

NEW QUESTION: 4
A recommended change to enhance detection methodology includes: (Choose two)
A. Ignoring the need for employee cybersecurity awareness training
B. Simplifying the cybersecurity toolset to a single solution
C. Regularly updating and testing the incident response plan
D. Enhancing data collection and normalization processes
Answer: (SHOW ANSWER)

NEW QUESTION: 5
In threat intelligence handling, cataloging is important for:
A. Increasing the speed of the internet connection
B. Reducing the size of the IT department
C. Ensuring compatibility with legacy systems
D. Making intelligence easily accessible for analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Memory-resident attacks can be analyzed using which tool?
A. Nmap
B. Wireshark
C. Volatility
D. Nessus
Answer: (SHOW ANSWER)

NEW QUESTION: 7
To identify unknown gaps in detection, one should:
A. Assume all configurations are secure
B. Conduct regular security assessments
C. Only trust verified threats
D. Rely solely on automated alerts
Answer: (SHOW ANSWER)

NEW QUESTION: 8
A runbook or playbook for a detectable scenario should include:
A. Corporate holiday schedules
B. The CEO's contact information
C. Steps for containment, eradication, and recovery
D. A list of favorite employee lunch spots
Answer: (SHOW ANSWER)

NEW QUESTION: 9
The effectiveness of a threat hunt can be improved by:
A. Investing in continuous training for the security team
B. Only using free or built-in tools
C. Limiting documentation to save time
D. Ignoring alerts during off-hours
Answer: (SHOW ANSWER)

NEW QUESTION: 10
To improve the effectiveness of a threat hunt, it is recommended to:
A. Increase the coffee budget for the security team
B. Ignore low severity alerts
C. Utilize more automated tools and techniques
D. Only hunt for threats during business hours
Answer: (SHOW ANSWER)

NEW QUESTION: 11
What disadvantage does automation in security operations face?
A. It can replace human intuition and decision-making
B. It reduces the need for cybersecurity policies
C. It may struggle with new and unknown threats
D. It can identify all types of malware without updates
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which scripting language is commonly used for automating the data analysis in threat hunting?
A. Python
B. HTML
C. Java
D. C++
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Utilizing threat intelligence effectively means integrating it into _____ processes.
A. financial planning
B. defensive
C. marketing
D. hiring
Answer: (SHOW ANSWER)

NEW QUESTION: 14

A comprehensive playbook addresses which phases of incident response? (Choose two)
A. Budget planning
B. Detection
C. Recovery
D. Lunch break scheduling
Answer: (SHOW ANSWER)

NEW QUESTION: 15
In the context of the threat hunting process, what does the term "pivot" mean?
A. To rotate data points in a visualization
B. To move quickly from one hypothesis to another
C. To confirm a suspected threat
D. To backtrack and analyze previous data
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Enhancing a detection methodology could involve:
A. Incorporating user and entity behavior analytics (UEBA)
B. Eliminating the review of false positives
C. Reducing the frequency of updates to the threat intelligence database
D. Focusing exclusively on historical data
Answer: (SHOW ANSWER)

NEW QUESTION: 17
During the investigation phase of the threat hunting process, what activity is typically conducted?
A. Mitigating the threat
B. Refining hypotheses
C. Collecting additional data
D. Generating threat intelligence reports
Answer: (SHOW ANSWER)

NEW QUESTION: 18

Constructing a signature for detection involves:
A. Calculating the downtime caused by an attack
B. Predicting future attack vectors
C. Identifying unique patterns of attack
D. Estimating the cost of an attack
Answer: (SHOW ANSWER)

NEW QUESTION: 19
The effectiveness of threat modeling techniques is enhanced by:
A. Limiting access to threat intelligence
B. Using a single threat intelligence source
C. Focusing solely on internal threats
D. Integrating diverse data sources for a comprehensive view
Answer: (SHOW ANSWER)

NEW QUESTION: 20
What does the term "honeypot" refer to in threat hunting techniques?
A. A decoy system designed to lure attackers
B. A tool used for network mapping
C. A type of encryption algorithm
D. A sweet treat for security analysts
Answer: (SHOW ANSWER)

NEW QUESTION: 21
How does multiproduct integration enhance data visibility within a product?
A. By accelerating data deletion processes
B. By reducing the overall data storage needs
C. By limiting data access to senior management
D. By aggregating and correlating data across platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 22
A technique often used by advanced persistent threat actors that can be identified through log analysis is:
A. Using common software for tasks
B. Spear-phishing for initial access
C. Regularly patching vulnerabilities
D. Encrypting all data stored on servers
Answer: (SHOW ANSWER)

NEW QUESTION: 23

Security countermeasures should:
A. Be layered and comprehensive
B. Prioritize aesthetic considerations
C. Rely on security through obscurity
D. Only focus on perimeter defenses
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Structured threat hunting differs from unstructured threat hunting in that it:
A. Requires predefined datasets for analysis
B. Is based on specific hypotheses or indicators
C. Does not require any prior knowledge of threats
D. Is more ad hoc and relies on the hunter's intuition
Answer: (SHOW ANSWER)

NEW QUESTION: 25
For detecting memory-resident malware, it's essential to analyze:
A. USB device history
B. Disk storage allocation
C. Cloud storage access logs
D. Memory allocation patterns
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What is the primary goal of threat hunting?
A. To prevent users from accessing malicious websites
B. To create legal reports for compliance
C. To proactively find and mitigate potential threats before they cause harm
D. To install antivirus software on all endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Interpreting a threat intelligence report requires understanding of:
A. The legal implications of the attacker's actions
B. Only the technical details of the reported vulnerabilities
C. The context, including tactics, techniques, and procedures used by attackers
D. The financial impact of potential breaches
Answer: (SHOW ANSWER)

NEW QUESTION: 28
IoT device threat analysis must include: (Choose two)

A. Application behavior analysis
B. Analyzing the operating system's security features
C. Checking for updates to the device firmware
D. Reviewing the device's physical security mechanisms
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Techniques used by threat actors can be identified by analyzing:
A. The sequence of commands executed after initial compromise
B. The encryption algorithm of ransomware
C. The color scheme of the phishing email
D. The geographical location of the attacker
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Effective communication of threat hunting findings should:
A. Be tailored to the technical level of the audience
B. Focus only on the technical aspects, ignoring business impacts
C. Use technical language to demonstrate expertise
D. Prioritize sharing successes over lessons learned from failures
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Changes to a detection methodology to augment analytical and process gaps might include: (Choose two)
A. Relying solely on signature-based detection
B. Implementing behavioral analysis techniques
C. Decreasing the use of automation and machine learning
D. Integrating threat intelligence feeds
Answer: (SHOW ANSWER)

NEW QUESTION: 32

Memory-resident malware detection is challenging because:
A. It does not modify disk-based files
B. It only activates during a full moon
C. It can be easily detected with traditional antivirus
D. It requires physical access to the server
Answer: (SHOW ANSWER)

NEW QUESTION: 33
A mitigation strategy for blocking C2 traffic that involves analyzing behavioral patterns is known as:
A. Increasing network bandwidth
B. Whitelisting all inbound connections
C. Disabling network monitoring tools
D. Deploying anomaly-based detection
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Determining the priority level of attacks with the Cyber Kill Chain requires understanding the attacker's:
A. Preferred programming language
B. Physical location
C. Educational background
D. Progression through attack stages
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Python scripts in threat hunting are used for:
A. Conducting online marketing campaigns
B. Managing employee records
C. Designing corporate websites
D. Automating detection and analysis tasks
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which step in the threat hunting process involves creating and executing queries to search for indicators of compromise?
A. Data Analysis
B. Data Enrichment
C. Data Collection
D. Data Processing
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Why is it important to document and communicate findings during the threat hunting process?
A. To ensure that all findings are thoroughly investigated
B. To maintain compliance with industry regulations
C. To keep sensitive information confidential
D. To share knowledge and improve overall security posture
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What is a key advantage of AI in cybersecurity?
A. It can predict future attacks with 100% accuracy
B. It completely replaces the need for human security analysts
C. It eliminates the need for security patches
D. It can analyze vast amounts of data to identify potential threats
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following is included in the Pyramid of Pain?
A. Hash values
B. Encryption algorithms
C. Firewall rules
D. Usernames
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Blocking C2 traffic effectively requires:
A. Assuming all internal network traffic is safe
B. Focusing on inbound traffic only
C. Ignoring encrypted traffic as it's secure by default
D. Analyzing network traffic for anomalies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Advancing in the Threat Hunting Maturity Model involves:
A. Lowering the bar for what constitutes a successful hunt
B. Keeping threat hunting findings within the team to maintain knowledge exclusivity
C. Increasing reliance on manual processes
D. Integrating threat hunting findings into broader security practices
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Reverse engineering is used to determine compromises by:
A. Interviewing the IT staff
B. Disassembling and examining the malware code
C. Analyzing the attacker's social media profiles
D. Reviewing firewall logs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Data interpreted from memory-specific tools can reveal:
A. The need for more RAM
B. The preferred memory brand of attackers
C. Upcoming memory sales
D. Evidence of code injection attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 44
A key aspect of recommending attack remediation strategies is:
A. Focusing solely on external threats
B. Ensuring they are the least disruptive to business operations
C. Making them as complex as possible
D. Ignoring the cost implications
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which tool is specifically designed for static analysis of executable files for vulnerabilities?
A. PE Checker
B. Metasploit
C. BURP Suite
D. OWASP ZAP
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Effective tools and configurations for detection should:
A. Be regularly updated and patched
B. Always be the most expensive option for effectiveness
C. Only include open-source solutions
D. Be chosen based on the security team's familiarity
Answer: (SHOW ANSWER)

NEW QUESTION: 47
The process of removing outdated threat intelligence involves:
A. Updating firewall rules
B. Reviewing and discarding no longer relevant data
C. Patching software vulnerabilities
D. Retraining machine learning models
Answer: (SHOW ANSWER)

NEW QUESTION: 48
The MITRE ATT&CK framework is primarily used for modeling:
A. Physical security measures
B. Threats using tactics, techniques, and procedures
C. Software development lifecycles
D. Business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 49
A tactic that indicates a sophisticated threat actor rather than a commodity malware campaign is:
A. Targeted spear-phishing emails
B. Use of widely available exploit kits
C. Scanning the internet for vulnerable servers
D. Posting threats on social media
Answer: (SHOW ANSWER)

NEW QUESTION: 50
An augmentation of the detection methodology may necessitate:
A. Discouraging proactive threat research
B. Decreasing the variety of data sources monitored
C. Relying more heavily on predefined threat signatures
D. Implementing a zero-trust architecture
Answer: (SHOW ANSWER)

NEW QUESTION: 51

What is the first step in determining attack tactics, techniques, and procedures using logs?

A. Identifying unusual outbound traffic

B. Reviewing the timestamp of entries

C. Analyzing login attempts

D. Correlating events across different log sources

Answer: (SHOW ANSWER)

NEW QUESTION: 52

What is a recommended mitigation strategy to block Command and Control (C2) traffic?

A. Reducing the use of encryption

B. Allowing all outbound traffic

C. Decreasing firewall security levels

D. Implementing stringent egress filtering

Answer: D (LEAVE A REPLY)

NEW QUESTION: 53

The PASTA method is used to:

A. Perform automated static analysis on software

B. Prepare Italian dishes in the company cafeteria

C. Prioritize assets based on their criticality

D. Conduct penetration testing on network infrastructure

Answer: (SHOW ANSWER)

NEW QUESTION: 54

The primary use of unstructured threat hunting is to:

A. Conduct compliance audits

B. Follow a strict set of rules for analysis

C. Develop security policies

D. Explore the network for anomalies without predefined hypotheses

Answer: (SHOW ANSWER)

NEW QUESTION: 55

Identifying memory-resident attacks often requires the use of:

A. Network sniffers

B. Memory analysis tools

C. Disk-based forensics tools

D. Antivirus software

Answer: (SHOW ANSWER)

NEW QUESTION: 56

Artifacts at which level of the Pyramid of Pain provide the most context about an attack but are also the most challenging to use for attribution?

A. IP addresses

B. TTPs

C. Domain names

D. File hashes

Answer: (SHOW ANSWER)

NEW QUESTION: 57

The use of MITRE CAPEC helps in:

A. Optimizing network traffic

B. Modeling common attack patterns for software

C. Managing HR processes

D. Designing user interfaces

Answer: (SHOW ANSWER)

NEW QUESTION: 58

When interpreting the tactics, techniques, and procedures of a threat actor, which of the following is most crucial?

A. The specific malware variant used

B. The pattern of lateral movement within the network

C. The time of day the attack occurred

D. The volume of data exfiltrated

Answer: (SHOW ANSWER)

NEW QUESTION: 59

When using the MITRE ATT&CK framework to model threats, changes in _____ are critical for understanding evolving attack strategies.

A. organizational policies

B. tactics, techniques, and procedures

C. encryption algorithms

D. software development methodologies

Answer: (SHOW ANSWER)

NEW QUESTION: 60

Which of the following best describes an advanced persistent threat (APT)?

A. A short-term financial fraud scheme

B. An opportunistic ransomware attack

C. A quickly evolving malware variant

D. A long-term, targeted attack campaign

Answer: (SHOW ANSWER)