Cisco.300-220.v2026-01-29.q179

Exam Code:	300-220
Exam Name:	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps
Certification Provider:	Cisco
Free Question Number:	179
Version:	v2026-01-29
# of views:	129
# of Questions views:	1790
https://www.freepdfdumps.com/Cisco.300-220.v2026-01-29.q179.html	

NEW QUESTION: 1
What is the main goal of threat actor attribution techniques in cybersecurity?
A. Tracing attacks back to the source
B. Creating secure passwords
C. Implementing firewalls
D. Identifying vulnerabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following is NOT a common threat modeling technique?
A. Social engineering assessment
B. Attack surface analysis
C. STRIDE model
D. Data flow diagrams
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
What is the purpose of using TTPs in threat actor attribution?
A. To identify the threat actor's password
B. To identify the threat actor's Tactics, Techniques, and Procedures
C. To identify the threat actor's location
D. To identify the threat actor's email address
Answer: (SHOW ANSWER)

NEW QUESTION: 4
In threat modeling, what does the STRIDE acronym stand for?
A. Standards, Techniques, Risk analysis, Incident response, Defensive measures, Evaluation
B. System, Treats, Risks, Identification, Defense, Evaluation
C. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
D. Security, Threat, Response, Incident, Detection, Evaluation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
What is a common technique used in threat hunting that involves analyzing historical data to identify anomalies or patterns that may indicate a security threat?
A. Log analysis
B. Behavioral analysis
C. Signature-based detection
D. Network traffic analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
Which phase of the threat hunting process involves comparing established indicators of compromise against network behaviors?
A. Hypothesis generation
B. Threat confirmation
C. Data analysis
D. Objective and scope
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
What does the term "honeypot" refer to in threat hunting techniques?
A. A type of encryption algorithm
B. A sweet treat for security analysts
C. A tool used for network mapping
D. A decoy system designed to lure attackers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
What is the primary goal of threat hunting outcomes?
A. Enhancing overall security posture
B. Responding to security incidents
C. Preventing future attacks

D. Identifying potential threats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
What is the primary goal of threat emulation in threat hunting techniques?
A. To monitor system logs for anomalies
B. To analyze malware payloads
C. To replicate attacker techniques to test defenses
D. To encrypt sensitive data
Answer: (SHOW ANSWER)

NEW QUESTION: 10
What role does Threat Intelligence play in Threat Actor Attribution?
A. Threat Intelligence only focuses on mitigation strategies
B. Threat Intelligence provides information and context about potential threat actors
C. Threat Intelligence can directly identify threat actors
D. Threat Intelligence is not useful for Threat Actor Attribution
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
In threat hunting techniques, what is the purpose of decoy systems?
A. To deceive attackers by providing false information
B. To restrict access to sensitive data
C. To analyze network traffic
D. To monitor system performance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
What role do key performance indicators (KPIs) play in the Threat Hunting Process?
A. To measure the effectiveness of threat hunters
B. To identify potential threats
C. To deploy security tools
D. To analyze existing threat intelligence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
What is a challenge often faced in threat actor attribution?
A. Lack of data
B. False Flags
C. Predicting future attacks
D. Clear identification

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What is the purpose of conducting binary analysis when utilizing threat hunting techniques?
A. To set up decoy systems to attract adversaries
B. To monitor network traffic for anomalies
C. To analyze the structure and behavior of suspicious files
D. To conduct memory forensics on compromised systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 15
True or False: Threat modeling techniques are only relevant during the initial development phase of a project.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
Which technique involves leveraging machine learning algorithms and AI to help identify anomalies and potential security threats?
A. Signature-based detection
B. Threat intelligence analysis
C. Behavioral analysis
D. Machine learning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
Which threat hunting technique focuses on analyzing network traffic to detect and prevent threats?
A. Packet capture analysis
B. YARA rule matching

C. Netflow analysis
D. Behavior-based detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
What is the role of DNS monitoring in threat hunting?
A. To conduct penetration tests on external systems
B. To analyze network traffic for patterns of malicious activity
C. To encrypt all DNS queries
D. To block access to certain websites
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which technique involves manually reviewing log files and analyzing them for signs of malicious activity?
A. Log file analysis
B. Incident response
C. Signature-based detection
D. Network traffic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following is a technique used in threat actor attribution that focuses on identifying commonalities in attack patterns?
A. Entity profiling
B. Behavioral analysis
C. Pattern recognition
D. Indicator of compromise
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which of the following statements best describes the concept of threat hunting in cybersecurity?
A. Threat hunting aims to prevent all cyber attacks from happening
B. Threat hunting is solely focused on network maintenance and optimization
C. Threat hunting is a reactive method used to respond to threats after they have occurred
D. Threat hunting involves actively searching for potential threats that may have evaded traditional security measures
Answer: (SHOW ANSWER)

NEW QUESTION: 22

What is the purpose of reconnaissance in the context of threat hunting?
A. Collecting evidence
B. Gathering information about the network and potential adversaries
C. Identifying potential threats
D. Monitoring network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 23
What technique focuses on understanding and predicting the behavior of threat actors in order to better anticipate their actions?
A. Signature-based detection
B. Log correlation
C. Behavioral analysis
D. Threat intelligence analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
What is the key difference between threat hunting and traditional cybersecurity measures?
A. Threat hunting involves actively searching for threats
B. Threat hunting is reactive
C. Threat hunting only focuses on known threats
D. Traditional cybersecurity measures are proactive
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Behavioral analysis applies machine learning algorithms to detect anomalies in what type of data?
A. Threat intelligence reports
B. Endpoint activity
C. Log files
D. Network traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
In the threat hunting process, what is the purpose of the data collection phase?
A. Refine strategies
B. Develop hypotheses
C. Analyze collected data
D. Identify potential threats
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which threat hunting technique involves setting up honeypots to attract and monitor malicious activity?
A. Honeypot deployment
B. Threat modeling
C. Incident response
D. Malware analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
What is the purpose of using network traffic analysis as a threat hunting technique?
A. To detect unusual patterns or anomalies in network traffic
B. To conduct penetration testing on the network
C. To monitor user activity on endpoints
D. To analyze log files for known threat signatures
Answer: (SHOW ANSWER)

NEW QUESTION: 29
What role does correlation play in threat hunting?
A. It blocks incoming traffic from suspicious IP addresses
B. It ensures that all identified threats are immediately blocked
C. It monitors user activity but does not correlate it with any other data
D. It connects various data points to identify potential threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
In threat actor attribution, what does IOA stand for?
A. Indicators of Attribution
B. Indicators of Acquaintance
C. Indicators of Attack
D. Indicators of Analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following is a key step in threat modeling techniques?
A. Developing secure code
B. Conducting user acceptance testing
C. Performing vulnerability scans
D. Identifying potential threats
Answer: (SHOW ANSWER)

NEW QUESTION: 32
What is the main difference between threat hunting and traditional security measures like firewalls and antivirus software?
A. Threat hunting is reactive, while traditional security measures are proactive
B. Threat hunting focuses on known threats, while traditional security measures focus on unknown threats
C. Threat hunting requires advanced technical skills, while traditional security measures are user- friendly
D. Threat hunting involves actively searching for threats, while traditional security measures wait for alerts
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
In the context of the threat hunting process, what is an indicator of compromise (IOC)?
A. Weaknesses in network defenses
B. Known malware signatures
C. Anomalies in system behavior
D. Threat intelligence reports
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
In threat hunting, what is the purpose of conducting malware analysis on suspicious files or samples?
A. To identify indicators of compromise and behavior patterns
B. To create new malware samples
C. To infect other systems on the network
D. To encrypt data on endpoints
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Which of the following activities is part of the threat hunting process?
A. Waiting for alerts from security tools

B. Proactively searching for indicators of compromise within the network
C. Installing antivirus software on all devices
D. Training employees on cybersecurity best practices
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
What technique involves searching for patterns or behaviors indicative of potential threats in network traffic logs?
A. Netflow analysis
B. Packet analysis
C. DNS analysis
D. SIEM analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which technique focuses on continuously monitoring and analyzing data to detect ongoing or potential security threats within a network?
A. Network traffic analysis
B. Continuous monitoring
C. Behavioral analysis
D. Signature-based detection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
What is the first step in the threat hunting process according to common methodologies?
A. Threat actor attribution
B. Data collection
C. Threat modeling
D. Hypothesis generation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Which phase of the threat hunting process involves applying threat intelligence and context to detected threats?
A. Remediation
B. Analysis
C. Attribution
D. Investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 40

Why is it important for cybersecurity professionals to stay current on evolving threat landscapes and attack techniques?
A. To maintain a high level of job satisfaction
B. To focus solely on known threats
C. To effectively detect and respond to emerging threats
D. To impress colleagues and supervisors
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
During which phase of the threat hunting process would you develop and test hypotheses based on collected data?
A. Reporting
B. Hypothesis generation
C. Strategy refinement
D. Data collection
Answer: (SHOW ANSWER)

NEW QUESTION: 42
How can threat actor attribution aid in threat hunting?
A. By preventing all types of cyber attacks
B. By launching offensive cyber operations
C. By identifying potential future targets
D. By providing insights into the threat actor's methods and behaviors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
What is the purpose of threat modeling in the context of cybersecurity?
A. Prioritizing cybersecurity risks
B. Designing secure systems
C. Identifying specific threats
D. Generating attack vectors
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
What is the main goal of threat hunting?
A. To install security tools on all network devices
B. To report all potential threats to the authorities
C. To proactively detect and respond to cyber threats
D. To wait for alerts from security tools
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
What is the purpose of using attack trees in threat modeling?
A. To model the potential pathways an attacker could take
B. To visualize the attack surface of a system
C. To simulate potential cyber attacks
D. To categorize different types of threats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
Why is threat hunting considered a proactive approach to cybersecurity?
A. Because it increases network speed and efficiency
B. Because it only focuses on threats that have already caused damage
C. Because it actively searches for threats that may have gone undetected by traditional methods
D. Because it relies on software to automatically detect threats
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following factors can help in identifying threat actors?
A. Malware signatures
B. IP addresses
C. All of the above
D. Tactics, Techniques, and Procedures (TTPs)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
What is the primary goal of threat modeling in cybersecurity?
A. Developing incident response plans
B. Identifying vulnerabilities
C. Prioritizing security controls
D. Conducting penetration testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
What is threat hunting in the context of cybersecurity?
A. A method of responding to cyber incidents after they occur
B. A passive approach to waiting for threats to be detected through alerts
C. A process of securing endpoints from potential threats
D. A process of proactively searching for cyber threats within an organization's network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
What is the ultimate goal of threat hunting in cybersecurity?
A. To reduce the number of false negatives
B. To identify threats before they materialize into security incidents
C. To solely focus on known threats
D. To wait for security alerts to trigger
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Which of the following techniques involves searching for indicators of compromise (IoC) in an organization's network?
A. NetFlow analysis
B. IoC scanning
C. Geolocation tracking
D. Hashing algorithms
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
How can threat hunting help improve an organization's overall security posture?
A. By providing insights into potential vulnerabilities and threats
B. By increasing the number of false positive alerts
C. By reducing the need for ongoing security monitoring
D. By automating the incident response process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
What is the purpose of proactively conducting threat hunting in a cybersecurity environment?
A. To respond to security incidents after they have already occurred.
B. To detect and neutralize threats that have bypassed traditional security measures.
C. To generate automated cybersecurity reports.
D. To install new antivirus software on all devices.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 54
What is the first step in the threat hunting process?
A. Defending against known attacks
B. Identifying potential threat indicators
C. Analyzing network traffic
D. Understanding the organization's environment and assets
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
In threat actor attribution, what is a common indicator used to link multiple attacks to a single actor?
A. IP address
B. SMTP server
C. DNS server
D. MAC address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which technique involves creating "honeypots" to divert and detect potential attackers?
A. Lateral movement tracking
B. Threat intelligence analysis
C. Endpoint monitoring
D. Deception technology
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
What role does data flow diagram play in threat modeling?
A. Identifying security controls
B. Evaluating network protocols
C. Conducting penetration testing
D. Mapping the flow of data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
What is the purpose of leveraging SIEM tools in threat hunting?
A. To monitor physical security of the organization
B. To consolidate and analyze logs from multiple sources
C. To block all potential threats automatically
D. To conduct network scans and penetration tests

Answer: B (LEAVE A REPLY)

NEW QUESTION: 59
During which phase of the threat hunting process would you analyze the collected data for signs of potential threats?
A. Investigation
B. Hypothesis generation
C. Data collection
D. Strategy refinement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
What is the purpose of OSINT in Threat Actor Attribution?
A. To gather information from public sources
B. To analyze network traffic
C. To secure cloud environments
D. To encrypt data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
How can threat hunting outcomes contribute to risk management within an organization?
A. By identifying and mitigating security risks
B. By creating more vulnerabilities
C. By ignoring potential threats
D. By increasing security alerts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
What is the primary objective of the investigation phase in the threat hunting process?
A. Collect more data
B. Develop new strategies
C. Validate hypotheses

D. Analyze collected data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Which of the following factors can help in attributing a cyber attack to a threat actor?
A. Time of day
B. Command and control infrastructure
C. Browser history
D. Type of encryption used
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Why is it important for organizations to have trained threat hunters?
A. Trained threat hunters do not add value to the security posture of an organization.
B. Trained threat hunters can eliminate all security threats in the network.
C. They can effectively detect and respond to sophisticated threats.
D. Organizations can save costs by not investing in threat hunting training.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
What is an example of a threat hunting technique?
A. Signature-based detection
B. Incident response
C. Indicator of compromise (IOC) analysis
D. Vulnerability scanning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
Why is sandboxing considered an effective threat hunting technique?
A. Because it monitors system performance
B. Because it isolates potentially malicious software
C. Because it eliminates the need for security patches
D. Because it focuses on compliance requirements
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Why is persistence an important factor in threat actor attribution?
A. It allows for tracking of attacker movements
B. It shows the level of sophistication of the attacker
C. It indicates the frequency of attacks
D. It determines the attacker's motive

Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
What is the primary goal of threat hunting?
A. Responding to security incidents
B. Patching vulnerabilities
C. Identifying false positives
D. Proactively searching for threats in the network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
What role does threat intelligence play in evaluating Threat Hunting Outcomes?
A. Threat intelligence is not relevant to threat hunting outcomes
B. Threat intelligence helps identify attack patterns and adversaries
C. Threat intelligence slows down the threat hunting process
D. Threat intelligence is primarily used for compliance purposes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
Indicators of compromise (IOCs) are important in threat actor attribution as they provide:
A. Contextual data on the attack
B. Attribution to specific threat actors
C. Clues or evidence of potential compromise
D. Generic information about attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 71
What is the purpose of the data processing phase in the threat hunting process?
A. To filter and normalize data for analysis
B. To prioritize threats based on severity
C. To enrich collected data with threat intelligence
D. To block malicious traffic at the perimeter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
During threat hunting, what is the key focus of threat intelligence?
A. Denying access to the network
B. Identifying potential threats
C. Responding to known threats
D. Predicting future threats
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
Which of the following is a method used for threat actor attribution based on language and cultural references?
A. Behavioral Analysis
B. Stylometry
C. Linguistic Analysis
D. Social Engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following is NOT a common technique used in threat hunting?
A. Anomaly detection
B. Signature-based detection
C. Behavioral analytics
D. Predicting the weather
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
In the context of threat actor attribution, what aspect of attribution focuses on understanding the cultural, social, and political factors that may influence an attacker's behavior?
A. Geopolitical analysis
B. Social engineering
C. Behavioral analysis
D. Linguistic analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
In the Threat Hunting Process, what does the Data Acquisition phase involve?
A. Collecting data on successful attacks
B. Formulating hypotheses
C. Analyzing network traffic
D. Data collection from various sources
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
What indicates a successful C2 communication detection using endpoint logs? (Choose two)
A. Increased outbound traffic to unknown IPs
B. High volume of encrypted data sent to known ports
C. Unusual process tree formations
D. Frequent system reboots
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following is an essential component of effective threat hunting outcomes?
A. Limited analysis
B. Avoiding documentation
C. Cross-team collaboration
D. Ignoring security incidents
Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
What threat actor attribution technique involves studying the code of malware to identify unique characteristics or patterns that could link it to a specific threat actor or group?
A. Signature Analysis
B. Yara Rules
C. Data Mining
D. Code Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which method is commonly used to create threat models in cybersecurity?
A. Attack surface analysis
B. Penetration testing
C. Compliance assessment
D. Root cause analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
During which phase of the threat hunting process would you prioritize potential threats based on severity and impact?

A. Data analysis
B. Threat response
C. Data collection
D. Hypothesis generation
Answer: (SHOW ANSWER)

NEW QUESTION: 82
What is an important consideration when using open-source intelligence for threat actor attribution?
A. The geographic location of the intelligence source
B. The accuracy and reliability of the information
C. The cost-effectiveness of the intelligence source
D. The real-time availability of intelligence data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
Which of the following is a common data source used in threat hunting?
A. Social media feeds
B. Customer reviews
C. HR databases
D. Security logs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following is NOT a common data source used in threat hunting?
A. Endpoint logs
B. Firewall logs
C. Customer feedback
D. Network logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
When using the MITRE ATT&CK framework to model threats, changes in _____ are critical for understanding evolving attack strategies.
A. software development methodologies
B. encryption algorithms
C. organizational policies
D. tactics, techniques, and procedures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 86

What is the final step in the Threat Hunting process?
A. Reporting
B. Investigation
C. Eradication
D. Containment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following is not a primary goal of threat actor attribution?
A. Share threat intelligence
B. Identify motivations and objectives
C. Prevent future attacks
D. Directly confront threat actors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
_____ involves proactively searching through networks to detect and isolate advanced threats that evade existing security solutions.
A. Compliance auditing
B. Software development
C. Network optimization
D. Threat hunting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
What is the key benefit of understanding threat actor attribution techniques?
A. Enhancing data privacy
B. Optimizing cloud storage
C. Strengthening incident response
D. Streamlining network operations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
During which step of the Threat Hunting Process do threat hunters typically use security tools like SIEMs and EDR?
A. Validating the hypothesis
B. Deploying security tools
C. Analyzing existing threat intelligence
D. Identifying potential threats
Answer: (SHOW ANSWER)

NEW QUESTION: 91
What is the purpose of setting up baselines in threat hunting?
A. To establish a point of reference for normal network activity
B. To ignore any suspicious behavior detected
C. To lock down access to critical systems
D. To only focus on external threats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
What is the first step in the threat hunting process?
A. Analyzing network traffic
B. Applying machine learning algorithms
C. Documenting findings
D. Defining objectives and scope
Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
When conducting threat hunting, which phase focuses on taking action to mitigate or neutralize identified threats?
A. Threat response
B. Threat confirmation
C. Hypothesis generation
D. Data analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
What is the primary goal of the data collection phase in the threat hunting process?
A. Identify potential threats
B. Prepare for threat response
C. Validate known threats
D. Assess the impact of threats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
Which technique involves using data analysis techniques to proactively hunt for potential security threats within a network?
A. Threat hunting
B. Signature-based detection
C. Behavioral analysis
D. Log analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
Which of the following is a potential benefit of successful threat hunting outcomes?
A. Reduced incident response times
B. Increased likelihood of successful cyber attacks
C. Lack of actionable threat intelligence
D. Limited visibility into the organization's security environment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
Which term describes the practice of actively searching for cyber threats within an environment?
A. Threat monitoring
B. Threat hunting
C. Threat sleeping
D. Threat ignoring
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What is the purpose of the Response phase in the Threat Hunting process?
A. To collect and analyze data
B. To develop a plan for eradication
C. To take actions to prevent the threat from spreading
D. To focus on root cause analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
What is the role of a threat hunter in an organization's cybersecurity strategy?
A. To respond to cyber incidents after they occur
B. To perform routine maintenance on cybersecurity tools
C. To report all suspicious activities to the authorities
D. To proactively detect and respond to cyber threats before they cause damage

Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following is a common outcome of threat hunting activities?
A. Providing information to build better defenses
B. Predicting future cyber attacks
C. Identifying all vulnerabilities in the network
D. Real-time threat blocking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
What is the main goal of using infrastructure analysis in threat actor attribution?
A. To identify the physical infrastructure used by the attacker
B. To analyze the structure and organization of the attacker's operations
C. To gather intelligence from open-source data
D. To track the command and control server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following is NOT a common threat modeling technique?
A. Attack trees
B. Kill chain analysis
C. SWOT analysis
D. DREAD model
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
In threat actor attribution, what does the term "False Flag" refer to?
A. A tactic where threat actors plant misleading evidence
B. A technique to disguise the origins of an attack
C. A marker indicating the exact location of a threat actor
D. A campaign run by threat actors on social media
Answer: (SHOW ANSWER)

NEW QUESTION: 104
In threat modeling, what does the "DREAD" model stand for?
A. Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
B. Data loss, Resource exhaustion, Access control, Denial of service, Disclosure
C. Defense, Resilience, Evasion, Attack, Denial
D. Detect, Response, Eliminate, Analyze, Deterrent
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which threat modeling technique involves identifying security controls and countermeasures to mitigate threats?
A. STRIDE model
B. Threat modeling matrix
C. SWOT analysis
D. Data flow diagrams
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which technique focuses on monitoring and analyzing the behavior of endpoints or devices within a network to identify potential security issues?
A. Endpoint logging
B. Network traffic analysis
C. Signature-based detection
D. Behavioral analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
What is the primary goal of threat hunting in cybersecurity?
A. To prevent all cyber attacks
B. To improve network speed
C. To identify and neutralize advanced threats
D. To increase the number of false positives
Answer: C (LEAVE A REPLY)

NEW QUESTION: 108
Which of the following attribution techniques involves identifying similarities between known threat actor tactics, techniques, and procedures (TTPs)?
A. TTP analysis
B. Behavioral analysis

C. Indicators of compromise (IoC) analysis
D. Cloud forensics
Answer: (SHOW ANSWER)

NEW QUESTION: 109
What is an example of a threat hunting technique?
A. Vulnerability scanning
B. Signature-based detection
C. Incident response
D. Indicator of compromise (IOC) analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
What is a common technique used in threat hunting to detect anomalies in network traffic?
A. Random password generation
B. Ignoring network traffic altogether
C. Manual inspection of all log files
D. Machine learning algorithms
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which technique involves monitoring network traffic for unusual or suspicious patterns that may indicate a potential threat?
A. Network traffic analysis
B. Signature-based detection
C. Endpoint logging
D. Behavioral analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
Which technique involves analyzing threat intelligence feeds and reports to better understand the tactics, techniques, and procedures of threat actors?
A. Signature-based detection
B. Behavioral analysis
C. Log correlation
D. Threat intelligence analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
How can threat hunting outcomes contribute to improving overall cybersecurity posture?
A. By withholding threat intelligence from the organization

B. By identifying and remediating vulnerabilities before they are exploited
C. By increasing the complexity of security systems
D. By ignoring potential threats to focus on other priorities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
When assessing Threat Hunting Outcomes, what are some common key performance indicators (KPIs) that may be used?
A. Time to detect and respond to incidents
B. All of the above
C. Number of security alerts generated
D. Number of system vulnerabilities identified
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
Which technique involves analyzing network traffic patterns to identify malicious activity?
A. SIEM correlation analysis
B. Network traffic analysis
C. Intrusion detection system
D. File integrity monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 116
In the context of threat hunting, what is the purpose of conducting "incubation"?
A. To directly confront threat actors
B. To deploy additional security controls
C. To observe the evolution of attack tactics
D. To slow down the attack process
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which of the following activities is a key component of threat hunting?
A. Waiting for threats to surface on their own
B. Proactively searching for suspicious activity
C. Logging in once a month to check for threats
D. Changing passwords daily
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
What is the primary goal of threat hunting outcomes?
A. To produce actionable intelligence to guide future defense strategies

B. To remove all existing threats from the network
C. To enhance the overall security posture of the organization
D. To identify all potential threats in the environment
Answer: (SHOW ANSWER)

NEW QUESTION: 119
What is Threat Actor Attribution?
A. Predicting future actions of threat actors
B. Identifying the motives of threat actors
C. Determining the geographical location of threat actors
D. Associating malicious activities with a specific threat actor
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
What is the role of hypothesis-driven hunting in threat hunting?
A. It relies solely on automated tools for threat detection.
B. It is not a common practice in threat hunting.
C. It involves randomly searching for threats without any specific goal.
D. It focuses on forming educated guesses about potential threats and testing them through investigation.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Which technique involves deploying a series of honey pots to lure attackers and gather information about their tactics?
A. Threat intelligence analysis
B. Network traffic analysis
C. Signature-based detection
D. Deception technology
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122

Which step in the threat modeling process involves considering what an attacker could do if they exploited a vulnerability?
A. Define the System
B. Mitigate Risks
C. Determine Vulnerabilities
D. Identify Threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 123
In threat hunting outcomes, what does an increase in the organization's security posture mean?
A. Decreased collaboration with security teams
B. Reduced number of security controls
C. Improved resilience to cyberattacks
D. Weakened security defenses
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
What is the purpose of using Maltego in threat actor attribution?
A. Correlate threat actor tactics and techniques
B. Visualize relationships between entities
C. Conduct open-source intelligence gathering
D. Analyze network traffic patterns
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which technique involves analyzing the digital artifacts left behind by threat actors in order to attribute cyber attacks?
A. Behavioral analysis
B. Digital forensics
C. Infrastructure analysis
D. Linguistic analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
What role does continuous monitoring play in the Threat Hunting Process?
A. It slows down the overall process
B. It is only important during the data collection phase
C. It helps in identifying potential threats before they escalate
D. It is not necessary
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
Which phase in the Threat Hunting Process focuses on leveraging intel to drive the investigation process?
A. Investigation and Validation
B. Data Analysis
C. Data Acquisition
D. Hypothesis Generation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Which phase of the Threat Hunting process involves identifying all potential security incidents?
A. Investigation
B. Containment
C. Eradication
D. Detection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 129
What is the typical role of a threat hunter in a cybersecurity team?
A. Reacting to incidents after they occur
B. Managing network communication
C. Developing software applications
D. Conducting proactive investigations to identify threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
Behavioral analysis in threat actor attribution involves understanding the tactics, techniques, and procedures (TTPs) used by threat actors, as well as:
A. Anomalies or patterns in behavior
B. Geolocation data
C. Network traffic patterns
D. Encryption methods
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
How does threat hunting contribute to improving a company's cybersecurity posture?
A. By eliminating all security vulnerabilities in the network
B. By providing a proactive approach to threat detection and response
C. By increasing employee productivity

D. By blocking all network traffic to prevent threats
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
What is a key benefit of implementing threat hunting in an organization's cybersecurity strategy?
A. Faster response time to threats in the network
B. Improved employee morale
C. Increased network downtime
D. Reduced need for employee training on cybersecurity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following techniques is used to group threat actors based on their relationships and affiliations?
A. Malware analysis
B. Social network analysis
C. Traffic analysis
D. Cognitive analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 134
What is one drawback of relying solely on technical indicators for threat actor attribution?
A. Underestimating the sophistication of the threat actor
B. Ignoring the motivation behind the attack
C. Failing to consider human behavior and tactics
D. Overestimating the capabilities of the threat actor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
What is the main goal of threat intelligence analysis as a threat hunting technique?
A. To monitor network traffic
B. To gather information about potential threats
C. To identify vulnerabilities
D. To conduct penetration testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
Which level of the Pyramid of Pain is most difficult for attackers to change and adapt to when detected?
A. TTPs (Tactics, Techniques, and Procedures)

B. IP addresses
C. Hash values
D. Domain names
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which of the following is not a common indicator used in threat actor attribution?
A. Email address
B. Employee age
C. IP address
D. MAC address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
What is the difference between threat hunting and incident response?
A. Threat hunting is automated, while incident response is manual
B. Threat hunting is proactive, while incident response is reactive
C. Threat hunting is only performed by external security vendors, while incident response is handled internally
D. Threat hunting focuses on identifying and mitigating threats, while incident response focuses on containment and recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Why is data collection crucial in threat hunting?
A. Data collection is not necessary in threat hunting.
B. It provides valuable information for investigating potential threats.
C. Data collection is solely the responsibility of threat hunters.
D. It slows down the threat hunting process.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 140

What is the primary goal of threat hunting in cybersecurity?
A. To analyze trends and patterns in network traffic
B. To prevent all cyber attacks
C. To quickly respond to incidents after they occur
D. To proactively identify and mitigate threats before they cause harm
Answer: (SHOW ANSWER)

NEW QUESTION: 141
What role does threat intelligence play in the context of threat hunting?
A. Threat intelligence focuses on network speed and performance
B. Threat intelligence is used to identify known threats and indicators of compromise
C. Threat intelligence only includes information on physical security threats
D. Threat intelligence is not relevant to threat hunting
Answer: (SHOW ANSWER)

NEW QUESTION: 142
What is the final step in the threat hunting process?
A. Analysis
B. Attribution
C. Reporting
D. Remediation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
What is the primary focus of the STRIDE threat modeling technique?
A. Attack Trees
B. Threat classification based on six categories
C. Security design principles
D. Data Flow Diagrams
Answer: (SHOW ANSWER)

NEW QUESTION: 144
What is the primary goal of conducting threat hunting in a cybersecurity environment?
A. Eliminating all false positives
B. Preventing all future cyber attacks
C. Identifying external threats
D. Enhancing overall security posture
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145

In threat hunting, what is the purpose of conducting memory forensics on compromised systems?
A. To identify running processes and network connections
B. To uninstall malicious software
C. To block network traffic
D. To recover deleted files
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
What is OSINT in the context of threat actor attribution?
A. Open Security Incident Notification
B. Open Source Intelligence
C. Operating System Intelligence
D. Outbound Security Investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 147
What is the final step in the Threat Hunting Process?
A. Investigation and Validation
B. Data Analysis
C. Hypothesis Generation
D. Data Acquisition
Answer: A (LEAVE A REPLY)

NEW QUESTION: 148
What social media platforms are commonly analyzed as part of open-source intelligence for threat actor attribution?
A. Instagram
B. Facebook
C. Twitter
D. LinkedIn
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following is NOT a step in the Elevation of Privilege (EoP) threat model technique?
A. Assessing potential privilege escalation scenarios
B. Identifying potential attack surfaces
C. Analyzing the impact of security vulnerabilities
D. Identifying trust boundaries
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
What is the first step in the threat hunting process?
A. Identifying potential threats
B. Developing threat models
C. Analyzing log files
D. Initiating incident response procedures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following is NOT a commonly used technique for threat actor attribution?
A. Data encryption
B. Behavioral analysis
C. Social media analysis
D. Threat intelligence sharing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 152
Which step in the threat hunting process focuses on creating a plan to respond to identified threats?
A. Data collection
B. Investigation
C. Hypothesis generation
D. Strategy refinement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 153
In the Threat Hunting Process, what step involves proactively searching for indicators of compromise (IoCs)?
A. Identifying potential threats
B. Threat hunting activity
C. Analyzing existing threat intelligence

D. Deploying security tools
Answer: B (LEAVE A REPLY)

NEW QUESTION: 154
Which of the following types of analysis is commonly used to track financial transactions and money flow in threat actor attribution?
A. Financial analysis
B. Emergency response analysis
C. Forensic analysis
D. Linguistic analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155
A comprehensive playbook addresses which phases of incident response? (Choose two)
A. Lunch break scheduling
B. Recovery
C. Budget planning
D. Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Endpoint artifacts are crucial for uncovering undetected threats. Which of the following are considered endpoint artifacts? (Choose two)
A. Bash history in Linux
B. DNS server logs
C. Windows Registry keys
D. Router configuration files
Answer: (SHOW ANSWER)

NEW QUESTION: 157
What is the goal of using "Endpoint Analysis" as a threat hunting technique?
A. to scan for vulnerabilities on network devices
B. to analyze data collected from endpoints
C. to monitor network traffic
D. to simulate phishing attacks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
Which of the following is NOT a typical outcome of successful threat hunting?
A. Guaranteed prevention of all cyber threats
B. Improved incident response capabilities

C. Increased visibility into the security landscape
D. Identification of new threat indicators
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
Which of the following is a key benefit of incorporating threat hunting into a cybersecurity strategy?
A. Reduced need for security training
B. Increased vulnerability to cyber attacks
C. Improved network speed and performance
D. Enhanced threat intelligence and visibility
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
How can threat hunting contribute to improving an organization's overall security posture?
A. By outsourcing threat hunting to third-party vendors
B. By relying solely on external security measures like firewalls and antivirus software
C. By ignoring potential threats to focus on more pressing issues
D. By proactively detecting and responding to threats before they escalate
Answer: D (LEAVE A REPLY)

NEW QUESTION: 161
What is the purpose of using "sandboxing" as a threat hunting technique?
A. To hide critical assets from potential attackers
B. To establish secure communication channels for threat intelligence
C. To encrypt data at rest and in transit
D. To isolate malicious files and observe their behavior
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
Which step in the threat hunting process involves creating and executing queries to search for indicators of compromise?
A. Data Collection
B. Data Processing
C. Data Enrichment
D. Data Analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following is NOT a common threat modeling technique?
A. Attack Tree

B. Abuse Case
C. Penetration Testing
D. Data Flow Diagram
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
How can Threat Actor Attribution help in improving incident response?
A. By providing information on the tools and techniques used by threat actors
B. By ignoring threat actors' activities
C. By increasing the attack surface
D. By blocking all network traffic immediately
Answer: (SHOW ANSWER)

NEW QUESTION: 165
What role do threat intelligence feeds play in the Threat Hunting Process?
A. They are not relevant
B. They provide valuable information on potential threats
C. They only work for specific types of threats
D. They slow down the process
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
What is Threat Actor Attribution?
A. The act of identifying a threat actor's motivation
B. The act of identifying a threat actor's name
C. The act of identifying a threat actor's email address
D. The act of identifying a threat actor's location
Answer: (SHOW ANSWER)

NEW QUESTION: 167
What does the DREAD model assess in threat modeling?
A. Impact

B. Probability
C. Vulnerability
D. All of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following is a method used in threat actor attribution?
A. Geolocation tracking
B. Behavioral analysis
C. Social engineering
D. Packet sniffing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 169
Which of the following is a common endpoint-based threat hunting technique?
A. DNS monitoring
B. Firewall configuration
C. Network segmentation
D. Memory analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
Which threat modeling technique involves identifying potential threats by thinking like an attacker?
A. Attack surface analysis
B. STRIDE model
C. DREAD model
D. Penetration testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 171
In the Threat Hunting process, what should be done after a potential threat is detected?
A. Eradicate the threat from the network
B. Notify the incident response team
C. Contain the threat immediately
D. Investigate further to confirm the threat
Answer: (SHOW ANSWER)

NEW QUESTION: 172
What role does threat intelligence play in the Threat Hunting process?
A. It is not relevant to Threat Hunting

B. It helps in defining assumptions
C. It is only useful in the Reporting phase
D. It provides context for potential threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 173
Which phase in the Threat Hunting Process involves examining the collected data for unusual patterns?
A. Data Acquisition
B. Data Analysis
C. Investigation and Validation
D. Hypothesis Generation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
When should a threat hunting team revisit their hypothesis during the process?
A. Before deploying security tools
B. Before analyzing existing threat intelligence
C. Throughout the entire process
D. After validating the hypothesis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 175
What is the goal of lateral movement analysis in threat hunting techniques?
A. To analyze network traffic patterns
B. To detect vulnerabilities in the system
C. To identify malicious payloads in the network
D. To trace the path of an attacker within the network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 176
What is the final step in the Threat Hunting Process?
A. Identifying potential threats
B. Analyzing existing threat intelligence
C. Documenting findings and lessons learned
D. Mitigating the threats
Answer: (SHOW ANSWER)

NEW QUESTION: 177
What is the purpose of using a sandbox environment in threat hunting?
A. To restrict access to sensitive information

B. To isolate and analyze potentially harmful files or code
C. To provide a safe space for employees to test new software
D. To punish malicious actors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 178
Which threat hunting technique involves creating custom YARA rules to detect specific malware families?
A. Signature-based detection
B. Threat intelligence sharing
C. Log analysis
D. Network traffic analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 179
What is an advantage of using behavioral analysis for threat actor attribution?
A. Allows for tracking of threat actors across different platforms
B. Provides real-time identification of threat actors
C. Offers insights into the motives and strategies of threat actors
D. Can be easily manipulated by threat actors
Answer: (SHOW ANSWER)