ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 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

Question: 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

Question: 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

Question: 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

Question: 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

Question: 6

How can threat hunting help improve an organization's overall security posture?

A. By increasing the number of false positive alerts
B. By providing insights into potential vulnerabilities and threats
C. By automating the incident response process
D. By reducing the need for ongoing security monitoring

Answer: B

Question: 7

What is the purpose of setting up baselines in threat hunting?

A. To lock down access to critical systems
B. To establish a point of reference for normal network activity
C. To ignore any suspicious behavior detected
D. To only focus on external threats

Answer: B

Question: 8

What is a common technique used in threat hunting to detect anomalies in network traffic?

A. Machine learning algorithms
B. Random password generation
C. Manual inspection of all log files
D. Ignoring network traffic altogether

Answer: A

Question: 9

How can threat hunting benefit from leveraging threat intelligence feeds?

A. By reducing the need for regular monitoring
B. By providing up-to-date information on emerging threats
C. By automating the threat hunting process entirely
D. By limiting the scope of investigations to known indicators

Answer: B

Question: 10

What is the significance of gaining visibility into the network as part of threat hunting?

A. It ensures that all threats are immediately neutralized
B. It allows for the detection of abnormal behavior or signs of compromise
C. It requires organizations to limit access to security logs
D. It prevents the need for continuous threat hunting efforts

Answer: B

Question: 11

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

A. Monitoring inbound and outbound network traffic
B. Waiting for alerts to trigger before taking action
C. Conducting regular vulnerability scans without analysis
D. Relying solely on automated threat detection tools

Answer: A

Question: 12

How can organizations establish a culture of threat hunting within their cybersecurity teams?

A. By avoiding collaboration with other departments
B. By providing regular training on threat hunting techniques
C. By discouraging proactive security measures
D. By isolating threat hunters from the rest of the team

Answer: B

Question: 13

What is the purpose of threat modeling in the context of cybersecurity?

A. Identifying specific threats
B. Prioritizing cybersecurity risks

C. Designing secure systems D. Generating attack vectors

Answer: B

Question: 14

Which of the following is an example of a threat modeling technique?

A. Attack surface analysis
B. Vulnerability scanning
C. Patch management
D. Intrusion detection

Answer: A

Question: 15

In threat modeling, what does the "DREAD" model stand for?

A. Detect, Response, Eliminate, Analyze, Deterrent
B. Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
C. Defense, Resilience, Evasion, Attack, Denial
D. Data loss, Resource exhaustion, Access control, Denial of service, Disclosure

Answer: B

Question: 16

Which threat modeling technique involves identifying potential threats by thinking like an attacker?

A. DREAD model
B. Attack surface analysis
C. STRIDE model
D. Penetration testing

Answer: D

Question: 17

What is the primary goal of using the STRIDE model in threat modeling?

A. Identify potential attacker motivations and goals B. Assess the impact of security vulnerabilities C. Identify potential threats and their characteristics D. Ensure the security of sensitive data

Answer: C

Question: 18

Which of the following is NOT a step in the Elevation of Privilege (EoP) threat model technique?

A. Identifying trust boundaries

B. Identifying potential attack surfaces
C. Analyzing the impact of security vulnerabilities
D. Assessing potential privilege escalation scenarios

Answer: C

Question: 19

What is the main goal of threat actor attribution techniques in cybersecurity?

A. Identifying vulnerabilities
B. Tracing attacks back to the source
C. Creating secure passwords
D. Implementing firewalls

Answer: B

Question: 20

Which factor is NOT typically considered in threat actor attribution?

A. Geopolitical tensions
B. Linguistic skills
C. Technical capabilities
D. Brand reputation

Answer: D

Question: 21

Which of the following is a method used in threat actor attribution?

A. Packet sniffing
B. Social engineering
C. Geolocation tracking
D. Behavioral analysis

Answer: C

Question: 22

How can threat actor attribution techniques help organizations improve their cybersecurity defenses?

A. By providing real-time threat intelligence
B. By identifying patterns of attack behavior
C. By implementing encryption
D. By increasing network bandwidth

Answer: B

Question: 23

What is the key benefit of understanding threat actor attribution techniques?

A. Enhancing data privacy
B. Strengthening incident response
C. Streamlining network operations
D. Optimizing cloud storage

Answer: B

Question: 24

Which of the following factors can help in attributing a cyber attack to a threat actor?

A. Time of day
B. Type of encryption used
C. Command and control infrastructure
D. Browser history

Answer: C

Question: 25

Why is persistence an important factor in threat actor attribution?

A. It indicates the frequency of attacks
B. It shows the level of sophistication of the attacker
C. It allows for tracking of attacker movements
D. It determines the attacker's motive

Answer: C

Question: 26

Which technique involves analyzing metadata and artifacts left behind by attackers to determine their identity?

A. Behavioral analysis B. Network forensics
C. Malware analysis
D. Digital footprint analysis

Answer: B

Question: 27

What role does threat actor attribution play in cyber threat intelligence?

A. Providing context for threat alerts B. Enforcing compliance regulations C. Enhancing network speed D. Optimizing server performance

Answer: A

Question: 28

In threat actor attribution, what is a common indicator used to link multiple attacks to a single actor?

A. IP address
B. MAC address
C. DNS server
D. SMTP server

Answer: A

Question: 29

What is the primary objective of threat actor attribution techniques?

A. Identifying vulnerable systems
B. Detecting intrusions
C. Tracing attacks to specific threat actors
D. Implementing access controls

Answer: C

Question: 30

What is one drawback of relying solely on technical indicators for threat actor attribution?

A. Overestimating the capabilities of the threat actor
B. Underestimating the sophistication of the threat actor
C. Failing to consider human behavior and tactics
D. Ignoring the motivation behind the attack

Answer: C

Question: 31

What is the primary goal of threat hunting techniques?

A. To respond to threats after they have already occurred
B. To proactively search for potential threats within an organization
C. To ignore potential threats and focus on other security measures
D. To rely solely on automated tools for threat detection

Answer: B

Question: 32

Which of the following is a common technique used in threat hunting?

A. Network segmentation
B. Incident response
C. Cloud computing
D. Endpoint monitoring

Answer: D

Question: 33

What is the purpose of using a sandbox environment in threat hunting?

A. To punish malicious actors
B. To isolate and analyze potentially harmful files or code
C. To provide a safe space for employees to test new software
D. To restrict access to sensitive information

Answer: B

Question: 34

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: 35

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: 36

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: 37

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: 38

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: 39

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: 40

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: 41

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: 42

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: 43

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: 44

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: 45

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: 46

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: 47

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: 48

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: 49

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: 50

What is the final step in the threat hunting process?

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

Answer: B

Question: 51

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

Question: 52

In the context of the threat hunting process, what is an indicator of compromise (IOC)?

A. Weaknesses in network defenses
B. Anomalies in system behavior
C. Known malware signatures
D. Threat intelligence reports

Answer: C

Question: 53

Which phase of the threat hunting process involves applying threat intelligence and context to detected threats?

A. Analysis Investigation Attribution Remediation
B.
C. **Answer: C**
D.

Question: 54

What is the goal of the containment phase in the threat hunting process?

A. Identify potential vulnerabilities
B. Isolate affected systems
C. Analyze threat indicators
D. Create incident reports

Answer: B

Question: 55

What is the primary goal of conducting threat hunting in a cybersecurity environment?

A. Identifying external threats
B. Eliminating all false positives

C. Enhancing overall security posture
D. Preventing all future cyber attacks

Answer: C

Question: 56

Which of the following is NOT a common outcome of successful threat hunting activities?

A. Improved incident response capabilities
B. Decreased network visibility
C. Enhanced knowledge of the threat landscape
D. Reduction in dwell time of threats

Answer: B

Question: 57

What is the significance of threat hunting outcomes in the context of cybersecurity operations?

A. They provide evidence for compliance purposes
B. They help in assigning blame to specific threat actors
C. They contribute to building a proactive defense strategy
D. They solely focus on post-incident analysis

Answer: C

Question: 58

Which of the following best describes the concept of "threat intelligence" in the context of threat hunting outcomes?

A. Reactive approach to incident response
B. Analysis of adversary tactics, techniques, and procedures
C. Ignoring data from past cyber incidents
D. Strictly focusing on perimeter defense

Answer: B

Question: 59

What role does threat hunting play in achieving business objectives through improved outcomes?

A. Deterring all cyber attacks successfully
B. Streamlining incident response processes
C. Neglecting the importance of threat intelligence
D. Enabling better risk management decisions

Answer: D

Question: 60

Why is it crucial for cybersecurity teams to understand and analyze threat hunting outcomes regularly?

A. To increase false positives in the detection process
B. To allocate more resources to perimeter defense
C. To detect trends and patterns in cyber threats
D. To avoid sharing threat intelligence with stakeholders

Answer: C

Question: 61

What is the primary goal of threat hunting in cybersecurity?

A. To detect and respond to active threats
B. To prevent all cyber attacks from happening
C. To increase network speed and efficiency
D. To improve employee training on cybersecurity best practices

Answer: A

Question: 62

What is a common method used in threat hunting to search for unknown threats within a network?

A. Reactive monitoring
B. Proactive monitoring
C. Installing firewalls
D. Running regular vulnerability scans

Answer: B

Question: 63

What is the difference between threat hunting and traditional security measures like firewalls and antivirus software?

A. Threat hunting focuses on identifying threats that have evaded traditional security measures
B. Traditional security measures are more expensive than threat hunting
C. Threat hunting uses artificial intelligence while traditional security measures do not
D. Threat hunting is only used in government agencies, while traditional measures are used in private companies

Answer: A

Question: 64

When conducting threat hunting, what should cybersecurity professionals prioritize?

A. Identifying and remediating all vulnerabilities in the network B. Identifying and responding to active threats in the network C. Monitoring network traffic for compliance purposes D. Conducting regular security training for employees

Answer: B

Question: 65

Why is threat hunting considered a proactive approach to cybersecurity?

A. Because it relies on software to automatically detect threats
B. Because it actively searches for threats that may have gone undetected by traditional methods
C. Because it only focuses on threats that have already caused damage
D. Because it increases network speed and efficiency

Answer: B

Question: 66

During threat hunting, what is the key focus of threat intelligence?

A. Predicting future threats
B. Identifying potential threats
C. Responding to known threats
D. Denying access to the network

Answer: B

Question: 67

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 blocking all network traffic to prevent threats
D. By increasing employee productivity

Answer: B

Question: 68

What role does data analysis play in threat hunting?

A. Data analysis is not important in threat hunting
B. Data analysis helps identify patterns and anomalies that indicate potential threats
C. Data analysis only serves to slow down the threat hunting process
D. Data analysis is only used for compliance purposes

Answer: B

Question: 69

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 a reactive method used to respond to threats after they have occurred
C. Threat hunting involves actively searching for potential threats that may have evaded traditional security measures
D. Threat hunting is solely focused on network maintenance and optimization

Answer: C

Question: 70

Why is it important for cybersecurity professionals to understand the techniques used by threat actors?

A. To collaborate with threat actors for better network security
B. To become threat actors themselves
C. To identify and defend against threat actors effectively
D. To ignore threat actors in favor of traditional security measures

Answer: C

Question: 71

What is a key benefit of implementing threat hunting in an organization's cybersecurity strategy?

A. Reduced need for employee training on cybersecurity
B. Faster response time to threats in the network
C. Increased network downtime

D. Improved employee morale

Answer: B

Question: 72

What is the purpose of proactively conducting threat hunting in a cybersecurity environment?

A. To detect and neutralize threats that have bypassed traditional security measures.
B. To respond to security incidents after they have already occurred.
C. To install new antivirus software on all devices.

D. To generate automated cybersecurity reports.

Answer: A

Question: 73

What is the primary goal of threat modeling in cybersecurity?

A. Identifying vulnerabilities
B. Conducting penetration testing
C. Developing incident response plans
D. Prioritizing security controls

Answer: A

Question: 74

Which of the following is NOT a common threat modeling technique?

A. Attack trees
B. DREAD model
C. Kill chain analysis
D. SWOT analysis

Answer: D

Question: 75

In threat modeling, what does the DREAD model help organizations assess?

A. Hardware vulnerabilities
B. Financial risk
C. Severity of threats
D. Network bandwidth limitations

Answer: C

Question: 76

Which threat modeling technique involves mapping out the steps an attacker would take to compromise a system?

A. Kill chain analysis B. Risk assessment C. Data flow diagrams D. Root cause analysis

Answer: A

Question: 77

What is the purpose of using attack trees in threat modeling?

A. To visualize the attack surface of a system
B. To categorize different types of threats
C. To simulate potential cyber attacks
D. To model the potential pathways an attacker could take

Answer: D

Question: 78

Which threat modeling technique involves identifying security controls and countermeasures to mitigate threats?

A. Data flow diagrams
B. Threat modeling matrix
C. SWOT analysis
D. STRIDE model

Answer: B

Question: 79

What is a common technique used for threat actor attribution in cybersecurity?

A. Endpoint detection and response
B. Network traffic analysis
C. Geopolitical analysis
D. Malware analysis

Answer: C

Question: 80

Which of the following is NOT a factor considered in threat actor attribution?

A. Motive
B. Infrastructure
C. Frequency of attacks
D. Attribution

Answer: C

Question: 81

When conducting threat actor attribution, what type of analysis is used to determine the geographic

location of the attacker?

A. Social media analysis
B. Geographical information system (GIS) analysis
C. Malware analysis
D. Linguistic analysis

Answer: B

Question: 82

Which of the following aspects is often considered in threat actor attribution based on linguistic analysis?

A. Language proficiency
B. Dialect
C. Syntax and grammar
D. All of the above

Answer: D

Question: 83

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 track the command and control server
C. To analyze the structure and organization of the attacker's operations
D. To gather intelligence from open-source data

Answer: C

Question: 84

In the context of threat actor attribution, which of the following is a method used to track the command and control server?

A. Sinkholing
B. Social engineering
C. Brute force attacks
D. Data exfiltration

Answer: A

Question: 85

Which of the following attribution techniques involves identifying similarities between known threat actor tactics, techniques, and procedures (TTPs)?

A. Indicators of compromise (IoC) analysis

B. Behavioral analysis
C. TTP analysis
D. Cloud forensics

Answer: C

Question: 86

When conducting threat actor attribution, what is the purpose of analyzing the motive behind an attack?

A. To identify specific vulnerabilities in the target
B. To determine the financial gain of the attacker
C. To understand the attacker's goals and intentions D. To track the spread of malware

Answer: C

Question: 87

Which of the following is NOT a commonly used technique for threat actor attribution?

A. Threat intelligence sharing
B. Social media analysis
C. Data encryption
D. Behavioral analysis

Answer: C

Question: 88

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. Linguistic analysis
D. Behavioral analysis

Answer: A

Question: 89

Which of the following types of analysis is commonly used to track financial transactions and money flow in threat actor attribution?

A. Forensic analysis
B. Linguistic analysis
C. Financial analysis
D. Emergency response analysis

Answer: C

Question: 90

Which technique involves analyzing the digital artifacts left behind by threat actors in order to attribute cyber attacks?

A. Linguistic analysis
B. Infrastructure analysis
C. Behavioral analysis
D. Digital forensics

Answer: D

Question: 91

What is an example of a threat hunting technique?

A. Signature-based detection
B. Vulnerability scanning
C. Indicator of compromise (IOC) analysis
D. Incident response

Answer: C

Question: 92

Which of the following is a network-based threat hunting technique?

A. Log analysis
B. Port scanning
C. Malware sandboxing
D. Traffic analysis

Answer: D

Question: 93

What is the purpose of threat intelligence in threat hunting techniques?

A. To collect data for compliance purposes
B. To predict future cyber attacks
C. To increase network bandwidth
D. To ensure data encryption

Answer: B

Question: 94

Which of the following is a common endpoint-based threat hunting technique?

A. DNS monitoring
B. Firewall configuration
C. Memory analysis
D. Network segmentation

Answer: C

Question: 95

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 monitor system performance
D. To analyze network traffic

Answer: A

Question: 96

Which threat hunting technique involves analyzing system logs for unusual or suspicious activity?

A. Payload analysis
B. Behavioral analytics
C. Log analysis
D. Threat emulation

Answer: C

Question: 97

What is the goal of lateral movement analysis in threat hunting techniques?

A. To identify malicious payloads in the network
B. To trace the path of an attacker within the network
C. To analyze network traffic patterns
D. To detect vulnerabilities in the system

Answer: B

Question: 98

Why is anomaly detection considered a proactive threat hunting technique?

A. Because it only reacts to identified threats

B. Because it relies on known IOCs
C. Because it detects deviations from normal behavior
D. Because it requires a response from the SOC

Answer: C

Question: 99

Which threat hunting technique focuses on analyzing network traffic to detect and prevent threats?

A. Behavior-based detection
B. YARA rule matching
C. Netflow analysis
D. Packet capture analysis

Answer: C

Question: 100

What is the primary goal of threat emulation in threat hunting techniques?

A. To replicate attacker techniques to test defenses
B. To encrypt sensitive data
C. To monitor system logs for anomalies
D. To analyze malware payloads

Answer: A

Question: 101

Why is sandboxing considered an effective threat hunting technique?

A. Because it eliminates the need for security patches
B. Because it isolates potentially malicious software
C. Because it focuses on compliance requirements
D. Because it monitors system performance

Answer: B

Question: 102

What is the main purpose of memory analysis in threat hunting techniques?

A. Identifying potential threats in real-time
B. Analyzing historical data for patterns
C. Detecting and investigating suspicious activities in volatile memory
D. Monitoring network traffic for anomalies

Answer: C

Question: 103

What is the first step in the Threat Hunting process?

A. Identifying potential threats
B. Collecting data
C. Defining assumptions
D. Analyzing the data

Answer: C

Question: 104

During the Threat Hunting process, what is the purpose of collecting data?

A. To identify potential threats
B. To analyze security logs
C. To confirm assumptions and hypotheses
D. To create reports for management

Answer: C

Question: 105

Which phase of the Threat Hunting process involves identifying all potential security incidents?

A. Detection
B. Investigation
C. Containment
D. Eradication

Answer: A

Question: 106

In the Threat Hunting process, what should be done after a potential threat is detected?

A. Contain the threat immediately
B. Notify the incident response team
C. Investigate further to confirm the threat
D. Eradicate the threat from the network

Answer: C

Question: 107

Which step in the Threat Hunting process involves analyzing the behavior of the detected threat?

A. Contain
B. Investigate
C. Eradicate
D. Report

Answer: B

Question: 108

What is the final step in the Threat Hunting process?

A. Containment B. Investigation C. Eradication
D. Reporting

Answer: D

Question: 109

During the Investigation phase of the Threat Hunting process, what is the primary focus?

A. Identifying false positives
B. Analyzing threat behavior
C. Implementing security controls
D. Logging incident details

Answer: B

Question: 110

Which stage of the Threat Hunting process involves taking actions to prevent the detected threat from spreading?

A. Investigation Containment Eradication Reporting
B.
C.
D.

Answer: B

Question: 111

In the Eradication phase of the Threat Hunting process, what is the main goal?

A. Identify all affected systems
B. Remove all traces of the threat
C. Update security policies
D. Report the threat to management

Answer: B

Question: 112

What role does threat intelligence play in the Threat Hunting process?

A. It helps in defining assumptions
B. It provides context for potential threats C. It is only useful in the Reporting phase D. It is not relevant to Threat Hunting

Answer: B

Question: 113

Why is continuous monitoring important in the Threat Hunting process?

A. To ensure all threats are eradicated B. To detect new threats in real-time C. To generate reports for management D. To prioritize investigation tasks

Answer: B

Question: 114

What is the purpose of the Response phase in the Threat Hunting process?

A. To collect and analyze data
B. To focus on root cause analysis
C. To take actions to prevent the threat from spreading
D. To develop a plan for eradication

Answer: C

Question: 115

What is the primary goal of threat hunting outcomes?

A. To identify all potential threats in the environment
B. To remove all existing threats from the network
C. To enhance the overall security posture of the organization
D. To produce actionable intelligence to guide future defense strategies

Answer: D

Question: 116

What role does threat hunting outcomes play in improving cybersecurity defenses?

A. It has no impact on cybersecurity defenses
B. It allows for a reactive approach to security incidents
C. It provides proactive defense by identifying and mitigating threats early
D. It focuses solely on incident response after a breach occurs

Answer: C

Question: 117

Why is it important for organizations to analyze and act on threat hunting outcomes?

A. To avoid regulatory fines
B. To identify the threat actors behind attacks
C. To improve their security posture and prevent future incidents
D. To increase the complexity of their network infrastructure

Answer: C

Question: 118

Which of the following is a common outcome of threat hunting activities?

A. Real-time threat blocking
B. Predicting future cyber attacks
C. Providing information to build better defenses
D. Identifying all vulnerabilities in the network

Answer: C

Question: 119

What role does threat hunting outcomes play in incident response?

A. It eliminates the need for incident response teams
B. It provides real-time incident detection and response capabilities
C. It does not impact incident response efforts
D. It provides insights and context to improve incident response efforts

Answer: D

Question: 120

How can threat hunting outcomes contribute to the overall cybersecurity strategy of an organization?

A. By increasing the attack surface
B. By providing in-depth threat intelligence for better decision-making
C. By slowing down security operations
D. By limiting the visibility into the network

Answer: B

Question: 121

What is the primary goal of threat hunting in cybersecurity?

A. To prevent all cyber attacks
B. To quickly respond to incidents after they occur
C. To proactively identify and mitigate threats before they cause harm
D. To analyze trends and patterns in network traffic

Answer: C

Question: 122

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

A. Network logs
B. Firewall logs
C. Customer feedback
D. Endpoint logs

Answer: C

Question: 123

What is the difference between threat hunting and incident response?

A. Threat hunting is proactive, while incident response is reactive
B. Threat hunting focuses on identifying and mitigating threats, while incident response focuses on containment and recovery
C. Threat hunting is automated, while incident response is manual
D. Threat hunting is only performed by external security vendors, while incident response is handled internally

Answer: B

Question: 124

How can threat hunting enhance an organization's cybersecurity posture?

A. By improving incident response times
B. By reducing false positives in security alerts
C. By identifying unknown threats that traditional security measures may miss
D. By providing real-time monitoring of network traffic

Answer: C

Question: 125

What is the main difference between threat hunting and traditional security measures like firewalls and antivirus software?

A. Threat hunting focuses on known threats, while traditional security measures focus on unknown threats
B. Threat hunting is reactive, while traditional security measures are proactive
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

Question: 126

Which of the following is a key benefit of incorporating threat hunting into a cybersecurity strategy?

A. Improved network speed and performance B. Increased vulnerability to cyber attacks C. Enhanced threat intelligence and visibility D. Reduced need for security training

Answer: C

Question: 127

What role does threat intelligence play in the context of threat hunting?

A. Threat intelligence is not relevant to threat hunting
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 focuses on network speed and performance

Answer: B

Question: 128

Why is it important for cybersecurity professionals to stay current on evolving threat landscapes and attack techniques?

A. To impress colleagues and supervisors
B. To focus solely on known threats
C. To maintain a high level of job satisfaction
D. To effectively detect and respond to emerging threats

Answer: D

Question: 129

What is the primary focus of threat hunting as compared to traditional security measures?

A. Identifying and mitigating threats before they cause harm
B. Overwhelming analysts with false positives
C. Relying solely on automated security tools
D. Reacting to incidents after they occur

Answer: A

Question: 130

Which of the following statements best describes the concept of threat hunting?

A. Threat hunting is a passive approach to cybersecurity

B. Threat hunting involves proactively searching for and remediating potential security threats
C. Threat hunting relies solely on automated security tools
D. Threat hunting focuses on responding to incidents in real-time

Answer: B

Question: 131

What is the ultimate goal of threat hunting in cybersecurity?

A. To wait for security alerts to trigger
B. To reduce the number of false negatives
C. To identify threats before they materialize into security incidents
D. To solely focus on known threats

Answer: C

Question: 132

What is the purpose of reconnaissance in the context of threat hunting?

A. Identifying potential threats
B. Collecting evidence
C. Gathering information about the network and potential adversaries
D. Monitoring network traffic

Answer: C

Question: 133

What is the main purpose of threat modeling in cybersecurity?

A. Identifying vulnerabilities
B. Assessing current threats
C. Quantifying risks
D. Evaluating security controls

Answer: A

Question: 134

Which method is commonly used to create threat models in cybersecurity?

A. Root cause analysis
B. Attack surface analysis
C. Penetration testing
D. Compliance assessment

Answer: B

Question: 135

What is the goal of asset identification in threat modeling?

A. Assessing system performance B. Identifying critical components C. Measuring security posture D. Analyzing attacker behavior

Answer: B

Question: 136

Which of the following is NOT a common threat modeling technique?

A. Data flow diagrams
B. STRIDE model
C. Attack surface analysis
D. Social engineering assessment

Answer: D

Question: 137

In threat modeling, what does the STRIDE acronym stand for?

A. System, Treats, Risks, Identification, Defense, Evaluation
B. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
C. Security, Threat, Response, Incident, Detection, Evaluation
D. Standards, Techniques, Risk analysis, Incident response, Defensive measures, Evaluation

Answer: B

Question: 138

Which step in threat modeling involves analyzing the impact of potential threats on system assets?

A. Attack surface analysis B. Software design review C. Threat assessment
D. Risk mitigation planning

Answer: C

Question: 139

Which of the following threat actor attribution techniques involves identifying patterns or anomalies in an attacker's behavior over time?

A. Behavioral Analysis
B. Code Analysis
C. Malware Analysis
D. Indicators of Compromise

Answer: A

Question: 140

Which threat actor attribution technique focuses on determining where an attack originated from by examining network traffic?

A. Open-Source Intelligence
B. IP Geolocation
C. Network Forensics
D. Hash Analysis

Answer: C

Question: 141

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. Code Analysis
B. Signature Analysis
C. Data Mining
D. Yara Rules

Answer: A

Question: 142

Which of the following is NOT a threat actor attribution technique?

A. Social Media Analysis
B. Indicators of Compromise
C. Open-Source Intelligence
D. Protocol Analysis

Answer: D

Question: 143

Open-source intelligence (OSINT) is commonly used in threat actor attribution to gather information from public sources such as:

A. Social Media
B. Internal Logs

C. Dark Web
D. Encrypted Messaging Apps

Answer: A

Question: 144

Which threat actor attribution technique involves examining cryptographic hashes of files to identify known malicious content or indicators?

A. Hash Analysis
B. Behavioral Analysis
C. Network Forensics
D. Code Analysis

Answer: A

Question: 145

What threat actor attribution technique focuses on analyzing the digital signatures or characteristics of malware to identify patterns or similarities?

A. Yara Rules
C. Signature Analysis
D. Data Mining
D. Network Forensics

Answer: B

Question: 146

Which of the following threat actor attribution techniques involves collecting and analyzing information from log files, network packets, and system snapshots to identify malicious activity?

A. Data Mining
B. Network Forensics
C. Protocol Analysis
D. Behavioral Analysis

Answer: B

Question: 147

Indicators of compromise (IOCs) are important in threat actor attribution as they provide:

A. Attribution to specific threat actors
B. Generic information about attacks
C. Contextual data on the attack

D. Clues or evidence of potential compromise

Answer: D

Question: 148

What social media platforms are commonly analyzed as part of open-source intelligence for threat actor attribution?

A. LinkedIn
B. Facebook
C. Twitter
E. Instagram

Answer: C

Question: 149

Behavioral analysis in threat actor attribution involves understanding the tactics, techniques, and procedures (TTPs) used by threat actors, as well as:

A. Geolocation data
B. Network traffic patterns
C. Anomalies or patterns in behavior
D. Encryption methods

Answer: C

Question: 150

Which threat actor attribution technique involves studying the motivation, goals, tactics, and techniques of known threat actor groups to identify similarities in their behavior?

A. Behavioral Analysis
B. Cyber Intelligence Analysis
C. Open-source Intelligence (OSINT)
D. Malware Analysis

Answer: A

Question: 151

What is the purpose of leveraging SIEM tools in threat hunting?

A. To block all potential threats automatically
B. To consolidate and analyze logs from multiple sources
C. To conduct network scans and penetration tests
D. To monitor physical security of the organization

Answer: B

Question: 152

Which of the following is a common technique used in threat hunting to identify anomalies in network traffic?

A. Network segmentation
B. Packet capturing
C. Signature-based detection
D. DNS monitoring

Answer: B

Question: 153

What is the primary goal of implementing endpoint detection and response solutions in threat hunting?

A. To encrypt all data on endpoints
B. To block all incoming network traffic
C. To monitor and respond to security incidents on endpoints
D. To control access to sensitive data

Answer: C

Question: 154

In threat hunting, what is the purpose of conducting memory forensics on compromised systems?

A. To recover deleted files
B. To identify running processes and network connections
C. To block network traffic
D. To uninstall malicious software

Answer: B

Question: 155

What is the benefit of using decoy systems in threat hunting?

A. To provide a distraction for threat actors
B. To slow down network traffic
C. To collect information on attacker tactics and techniques
D. To increase system performance

Answer: C

Question: 156

Which of the following threat hunting techniques involves analyzing historical incident data and indicators of compromise?

A. YARA rules
B. Threat intelligence feeds
C. Data correlation
D. Threat modeling

Answer: C

Question: 157

What is the purpose of leveraging threat intelligence feeds in threat hunting?

A. To monitor physical security
B. To remove malware from endpoints
C. To enrich security logs with information about known threats
D. To conduct social engineering attacks

Answer: C

Question: 158

Which threat hunting technique involves setting up honeypots to attract and monitor malicious activity?

A. Threat modeling
B. Honeypot deployment
C. Malware analysis
D. Incident response

Answer: B

Question: 159

In threat hunting, what is the purpose of conducting malware analysis on suspicious files or samples?

A. To create new malware samples
B. To infect other systems on the network
C. To identify indicators of compromise and behavior patterns
D. To encrypt data on endpoints

Answer: C

Question: 160

Which threat hunting technique involves employing YARA rules to identify specific patterns or signatures

in files or network traffic?

A. Endpoint monitoring
B. Threat actor attribution
C. YARA scanning D. Data correlation

Answer: C

Question: 161

What is the role of DNS monitoring in threat hunting?

A. To analyze network traffic for patterns of malicious activity
B. To conduct penetration tests on external systems
C. To encrypt all DNS queries
D. To block access to certain websites

Answer: A

Question: 162

What is the purpose of conducting binary analysis when utilizing threat hunting techniques?

A. To analyze the structure and behavior of suspicious files
B. To monitor network traffic for anomalies
C. To set up decoy systems to attract adversaries
D. To conduct memory forensics on compromised systems

Answer: A

Question: 163

What is the first step in the threat hunting process?

A. Analyzing network traffic
B. Defining objectives and scope
C. Documenting findings
D. Applying machine learning algorithms

Answer: B

Question: 164

During which phase of the threat hunting process would you conduct data analysis and review logs?

A. Objectives and scope
B. Hypothesis generation
C. Data collection
D. Data analysis

Answer: D

Question: 165

What is the purpose of hypothesis generation in the threat hunting process?

A. To validate known threats
B. To identify potential threats
C. To rule out false positives
D. To classify threat actors

Answer: B

Question: 166

Which phase of the threat hunting process involves leveraging threat intelligence and assessing the impact of potential threats?

A. Data analysis
B. Data collection
C. Hypothesis generation
D. Threat confirmation

Answer: D

Question: 167

When conducting threat hunting, which phase focuses on taking action to mitigate or neutralize identified threats?

A. Threat confirmation
B. Threat response
C. Hypothesis generation
D. Data analysis

Answer: B

Question: 168

What is the final step in the threat hunting process?

A. Documenting findings B. Objectives and scope C. Hypothesis generation D. Threat response

Answer: A

Question: 169

Which phase of the threat hunting process involves comparing established indicators of compromise against network behaviors?

A. Data analysis
B. Threat confirmation
C. Objective and scope
D. Hypothesis generation

Answer: B

Question: 170

What is the primary goal of the data collection phase in the threat hunting process?

A. Identify potential threats
B. Validate known threats
C. Prepare for threat response
D. Assess the impact of threats

Answer: A

Question: 171

Which phase of the threat hunting process involves setting clear goals and defining the scope of the hunt?

A. Data collection
B. Threat confirmation
C. Objectives and scope
D. Threat response

Answer: C

Question: 172

What is the purpose of the threat response phase in the threat hunting process?

A. To detect network anomalies
B. To validate identified threats
C. To take action on confirmed threats
D. To analyze gathered data

Answer: C

Question: 173

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

A. Data analysis
B. Data collection
C. Hypothesis generation
D. Threat response

Answer: D

Question: 174

What role does continuous monitoring play in the Threat Hunting Process?

A. It is not necessary
B. It is only important during the data collection phase
C. It helps in identifying potential threats before they escalate
D. It slows down the overall process

Answer: C

Question: 175

What is the primary goal of threat hunting outcomes?

A. To identify and mitigate all potential threats
B. To compile a list of known security vulnerabilities
C. To proactively detect and respond to threats
D. To create awareness about cybersecurity best practices

Answer: C

Question: 176

Which of the following is NOT a typical outcome of successful threat hunting?

A. Identification of new threat indicators
B. Improved incident response capabilities
C. Guaranteed prevention of all cyber threats
D. Increased visibility into the security landscape

Answer: C

Question: 177

How can threat hunting outcomes contribute to improving overall cybersecurity posture?

A. By identifying and remediating vulnerabilities before they are exploited
B. By ignoring potential threats to focus on other priorities
C. By increasing the complexity of security systems
D. By withholding threat intelligence from the organization

Answer: A

Question: 178

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. Limited visibility into the organization's security environment D. Lack of actionable threat intelligence

Answer: A

Question: 179

What role do threat hunting outcomes play in enhancing threat intelligence capabilities?

A. Threat hunting outcomes contribute significantly to decreasing threat intelligence quality
B. Threat hunting outcomes have no impact on threat intelligence capabilities
C. Threat hunting outcomes can enhance threat intelligence by providing valuable context and insights
D. Threat hunting outcomes only focus on historical data and do not provide actionable intelligence

Answer: C

Question: 180

How can threat hunting outcomes help organizations stay ahead of evolving cyber threats?

A. By ignoring potential threats to focus on other priorities
B. By minimizing visibility into the organization's security landscape
C. By proactively identifying and mitigating potential threats
D. By avoiding investing in cybersecurity technologies and tools

Answer: C

Question: 181

What is the primary goal of threat hunting in cybersecurity?

A. To prevent all cyber attacks
B. To identify and neutralize advanced threats
C. To increase the number of false positives
D. To improve network speed

Answer: B

Question: 182

Which of the following is NOT a common data source for threat hunting?

A. Network traffic logs
B. Endpoint detection and response data
C. Weather forecast data
D. Application logs

Answer: C

Question: 183

What is the typical role of a threat hunter in a cybersecurity team?

A. Reacting to incidents after they occur
B. Conducting proactive investigations to identify threats
C. Managing network communication
D. Developing software applications

Answer: B

Question: 184

Why is threat hunting important in cybersecurity?

A. It helps increase the number of false positives
B. It only focuses on known threats
C. It helps identify threats that may have evaded traditional security measures
D. It slows down network operations

Answer: C

Question: 185

Which term describes the practice of actively searching for cyber threats within an environment?

A. Threat monitoring
B. Threat ignoring
C. Threat hunting
D. Threat sleeping

Answer: C

Question: 186

What is the key difference between threat hunting and traditional cybersecurity measures?

A. Threat hunting only focuses on known threats
B. Traditional cybersecurity measures are proactive
C. Threat hunting is reactive
D. Threat hunting involves actively searching for threats

Answer: D

Question: 187

Which of the following is NOT a common technique used in threat hunting?

A. Signature-based detection
B. Anomaly detection
C. Behavioral analytics
D. Predicting the weather

Answer: D

Question: 188

How does threat hunting help organizations improve their cyber defense posture?

A. By ignoring all potential threats
B. By identifying and neutralizing advanced threats
C. By slowing down network operations
D. By increasing the number of false positives

Answer: B

Question: 189

Which of the following activities is a key component of threat hunting?

A. Waiting for threats to surface on their own
B. Logging in once a month to check for threats C. Proactively searching for suspicious activity D. Changing passwords daily

Answer: C

Question: 190

In threat hunting, what does the term "false positive" refer to?

A. A legitimate threat that has not been detected
B. A suspicious activity that turns out to be harmless
C. A weather forecast
D. A common cybersecurity tool

Answer: B

Question: 191

Which of the following best describes the mindset of a successful threat hunter?

A. Reactive and passive
B. Proactive and aggressive
C. Never taking action
D. Accepting all threats

Answer: B

Question: 192

What is the first step in the threat hunting process?

A. Analyzing network traffic

B. Identifying potential threat indicators
C. Defending against known attacks
D. Understanding the organization's environment and assets

Answer: D

Question: 193

What is an important step in threat modeling that involves identifying potential threats and their associated risks?

A. Defining security requirements
B. Identifying assets and their value
C. Conducting vulnerability assessments
D. Creating a threat matrix

Answer: B

Question: 194

Which of the following is a common approach used in threat modeling to identify potential attacker motivations and capabilities?

A. Data flow diagrams
B. STRIDE framework
C. DREAD model
D. Attack trees

Answer: C

Question: 195

In threat modeling, which of the following involves creating potential threat scenarios based on known vulnerabilities in a system?

A. Attack surface analysis
B. Risk assessment
C. Misuse case development
D. Threat modeling decomposition

Answer: A

Question: 196

Which threat modeling technique focuses on identifying abuse cases or scenarios where a system is misused for unauthorized purposes?

A. Threat modeling decomposition

B. Misuse case development
C. Attack surface analysis
D. Threat agent profiling

Answer: B

Question: 197

What is the primary goal of threat modeling in cybersecurity?

A. To eliminate all potential threats
B. To prioritize security controls
C. To identify and mitigate security risks
D. To predict future cyber threats

Answer: C

Question: 198

Which threat modeling technique involves breaking down a system into smaller components to analyze individual security concerns?

A. Misuse case development
B. Threat modeling decomposition
C. STRIDE framework mapping
D. Attack trees analysis

Answer: B

Question: 199

What is Threat Actor Attribution?

A. Identifying the motives of threat actors
B. Determining the geographical location of threat actors
C. Associating malicious activities with a specific threat actor
D. Predicting future actions of threat actors

Answer: C

Question: 200

Which of the following is an indicator commonly used for threat actor attribution?

A. IP address
B. Geolocation
C. User agent string
D. Malware hash

Answer: A

Question: 201

What is an advantage of using digital fingerprints for threat actor attribution?

A. Provides real-time tracking of threat actors
B. Allows for easy identification of threat actors
C. Can be easily modified by threat actors
D. Provides unique signatures for different threat actors

Answer: D

Question: 202

When analyzing threat actor behavior, what does TTP stand for?

A. Tactics, Tools, Procedures
B. Threat, Timing, Process
C. Targets, Techniques, Protocols
D. Tracking, Timeline, Patterns

Answer: A

Question: 203

Which of the following is a method used for threat actor attribution based on language and cultural references?

A. Linguistic Analysis
B. Stylometry
C. Behavioral Analysis
D. Social Engineering

Answer: A

Question: 204

What is an important consideration when using open-source intelligence for threat actor attribution?

A. The accuracy and reliability of the information
B. The cost-effectiveness of the intelligence source
C. The real-time availability of intelligence data
D. The geographic location of the intelligence source

Answer: A

Question: 205

Which of the following is a technique used in threat actor attribution that focuses on identifying commonalities in attack patterns?

A. Behavioral analysis
B. Entity profiling
C. Indicator of compromise
D. Pattern recognition

Answer: D

Question: 206

What is the purpose of establishing "personas" in threat actor attribution?

A. To create fictional characters to engage with threat actors
B. To track individual threat actors over time
C. To organize different threat actor groups based on characteristics
D. To simplify complex threat actor information for analysis

Answer: D

Question: 207

Which of the following techniques is used to group threat actors based on their relationships and affiliations?

A. Social network analysis
B. Cognitive analysis Malware analysis Traffic analysis
C.
D.

Answer: A

Question: 208

In threat actor attribution, what does IOA stand for?

A. Indicators of Analysis
B. Indicators of Attribution
C. Indicators of Attack
D. Indicators of Acquaintance

Answer: C

Question: 209

What is an advantage of using behavioral analysis for threat actor attribution?

A. Provides real-time identification of threat actors
B. Allows for tracking of threat actors across different platforms
C. Can be easily manipulated by threat actors
D. Offers insights into the motives and strategies of threat actors

Answer: D

Question: 210

What is the primary goal of threat actor attribution techniques?

A. Identifying network vulnerabilities
B. Identifying commonalities in attack patterns
C. Investigating employee behavior
D. Identifying phishing emails

Answer: B

Question: 211

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. Signature-based detection
B. Behavioral analysis
C. Network traffic analysis
D. Log analysis

Answer: D

Question: 212

Which technique involves monitoring network traffic for unusual or suspicious patterns that may indicate a potential threat?

A. Signature-based detection
B. Behavioral analysis
C. Network traffic analysis
D. Endpoint logging

Answer: C

Question: 213

What technique focuses on understanding and predicting the behavior of threat actors in order to better anticipate their actions?

A. Signature-based detection
B. Behavioral analysis
C. Threat intelligence analysis
D. Log correlation

Answer: B

Question: 214

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. Threat intelligence analysis
D. Log correlation

Answer: C

Question: 215

What technique involves correlating logs and data from various sources to identify potential security threats or breaches?

A. Signature-based detection
B. Behavioral analysis
C. Threat intelligence analysis
D. Log correlation

Answer: D

Question: 216

Which technique focuses on identifying known patterns or signatures of known threats within a network or system?

A. Signature-based detection
B. Behavioral analysis
C. Network traffic analysis
D. Endpoint logging

Answer: A

Question: 217

Which technique focuses on monitoring and analyzing the behavior of endpoints or devices within a network to identify potential security issues?

A. Signature-based detection
B. Behavioral analysis
C. Network traffic analysis
D. Endpoint logging

Answer: D

Question: 218

Which technique involves setting up decoy systems or honey pots to lure and observe potential threat actors in action?

A. Signature-based detection
B. Behavioral analysis
C. Deception techniques
D. Threat intelligence analysis

Answer: C

Question: 219

Which technique involves using data analysis techniques to proactively hunt for potential security threats within a network?

A. Signature-based detection
B. Behavioral analysis
C. Threat hunting
D. Log analysis

Answer: C

Question: 220

Which technique focuses on continuously monitoring and analyzing data to detect ongoing or potential security threats within a network?

A. Signature-based detection
B. Behavioral analysis
C. Continuous monitoring
D. Network traffic analysis

Answer: C

Question: 221

Which technique involves leveraging machine learning algorithms and AI to help identify anomalies and potential security threats?

A. Signature-based detection
B. Behavioral analysis
C. Machine learning
D. Threat intelligence analysis

Answer: C

Question: 222

What technique involves identifying and analyzing indicators of compromise (IOCs) to detect and respond to potential security incidents?

A. Behavioral Analytics
B. Indicator Analysis
C. Threat Intelligence Analysis
D. Network Traffic Analysis

Answer: B

Question: 223

What is the first step in the Threat Hunting Process?

A. Collecting Data
B. Analyzing Data
C. Identifying Anomalies
D. Formulating Hypotheses

Answer: A

Question: 224

During which phase of the Threat Hunting Process are potential threats investigated in depth?

A. Data Acquisition
B. Data Analysis
C. Hypothesis Generation
D. Investigation and Validation

Answer: D

Question: 225

Which step in the Threat Hunting Process involves using tools and methodologies to uncover potential threats?

A. Data Acquisition
B. Data Analysis
C. Hypothesis Generation
D. Investigation and Validation

Answer: C

Question: 226

What is the final step in the Threat Hunting Process?

A. Data Acquisition
B. Data Analysis
C. Hypothesis Generation
D. Investigation and Validation

Answer: D

Question: 227

In the Threat Hunting Process, what does the Data Acquisition phase involve?

A. Collecting data on successful attacks
B. Analyzing network traffic
C. Data collection from various sources
D. Formulating hypotheses

Answer: C

Question: 228

Which phase in the Threat Hunting Process involves examining the collected data for unusual patterns?

A. Data Acquisition
B. Data Analysis
C. Hypothesis Generation
D. Investigation and Validation

Answer: B

Question: 229

During Hypothesis Generation in the Threat Hunting Process, what do analysts form to guide their investigation?

A. Data sets
B. Patterns
C. Models
D. Hypotheses

Answer: D

Question: 230

In the Investigation and Validation phase of the Threat Hunting Process, what is done to confirm or refute the formed hypotheses?

A. More data collection
B. Detailed analysis
C. Testing against known attacks
D. Collaboration with external teams

Answer: C

Question: 231

Which phase in the Threat Hunting Process focuses on leveraging intel to drive the investigation process?

A. Data Acquisition
B. Data Analysis
C. Hypothesis Generation
D. Investigation and Validation

Answer: A

Question: 232

During the Threat Hunting Process, what is the goal of the Data Analysis phase?

A. Verify formed patterns
B. Identify anomalies
C. Gather more data
D. Formulate hypotheses

Answer: B

Question: 233

In the Threat Hunting Process, what step follows the identification of anomalies in the Data Analysis phase?

A. Data Acquisition
B. Hypothesis Generation
C. Investigation and Validation
D. Data Reanalysis

Answer: B

Question: 234

What is the purpose of the Hypothesis Generation phase in the Threat Hunting Process?

A. Forming initial conclusions based on gathered data
B. Creating a roadmap for the investigative process
C. Analyzing historical data for patterns
D. Correlating threat actor behavior with system logs

Answer: B

Question: 235

What is the primary goal of threat hunting outcomes?

A. Identifying potential threats
B. Preventing future attacks
C. Responding to security incidents
D. Enhancing overall security posture

Answer: D

Question: 236

In threat hunting outcomes, what is the value of documenting findings and lessons learned?

A. It is unnecessary
B. It helps in identifying trends and patterns
C. It slows down the investigation process
D. It is only useful for external reporting purposes

Answer: B

Question: 237

Which aspect of threat hunting outcomes involves improving incident response capabilities?

A. Analysis and investigation
B. Documentation and reporting
C. Proactive threat hunting
D. Post-mortem analysis

Answer: A

Question: 238

What is the benefit of sharing threat hunting outcomes with other teams within the organization?

A. It increases competition
B. It promotes collaboration and knowledge sharing
C. It leads to miscommunication
D. It is against security best practices

Answer: B

Question: 239

How can threat hunting outcomes contribute to risk management within an organization?

A. By ignoring potential threats
B. By increasing security alerts
C. By identifying and mitigating security risks
D. By creating more vulnerabilities

Answer: C

Question: 240

Which of the following is an essential component of effective threat hunting outcomes?

A. Ignoring security incidents B. Cross-team collaboration C. Avoiding documentation D. Limited analysis

Answer: B

Question: 241

What is threat hunting in the context of cybersecurity?

A. A process of proactively searching for cyber threats within an organization's network
B. A passive approach to waiting for threats to be detected through alerts
C. A process of securing endpoints from potential threats
D. A method of responding to cyber incidents after they occur

Answer: A

Question: 242

What is the main goal of threat hunting?

A. To wait for alerts from security tools
B. To proactively detect and respond to cyber threats
C. To install security tools on all network devices
D. To report all potential threats to the authorities

Answer: B

Question: 243

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

A. Firewall logs
B. Network traffic logs
C. Employee payroll records
D. Antivirus logs

Answer: C

Question: 244

What is the difference between threat hunting and traditional security measures like firewalls and antivirus software?

A. Threat hunting is reactive, while firewalls and antivirus software are proactive.
B. Threat hunting requires human intervention and intelligence gathering, while firewalls and antivirus software work automatically.
C. Threat hunting only focuses on external threats, while firewalls and antivirus software protect against both internal and external threats.
D. There is no difference, as threat hunting is just another term for traditional security measures.

Answer: B

Question: 245

Which of the following is an essential skill for a threat hunter?

A. Proficiency in a programming language
B. Proficiency in graphic design
C. Proficiency in database management
D. Proficiency in threat intelligence analysis

Answer: D

Question: 246

Why is collaboration with other security teams important in threat hunting?

A. It is not important, as threat hunting is an individual effort.
B. Collaboration allows for sharing of information and resources to better detect and respond to threats.
C. Collaboration slows down the threat hunting process.
D. Collaboration increases the risk of data breaches.

Answer: B

Question: 247

What is the importance of threat intelligence in threat hunting?

A. Threat intelligence provides real-time alerts to potential threats.
B. Threat intelligence allows threat hunters to anticipate and detect threats before they manifest.
C. Threat intelligence is not necessary for effective threat hunting.

D. Threat intelligence is only relevant for external threats, not internal threats.

Answer: B

Question: 248

Which of the following activities is part of the threat hunting process?

A. Waiting for alerts from security tools
B. Installing antivirus software on all devices
C. Proactively searching for indicators of compromise within the network
D. Training employees on cybersecurity best practices

Answer: C

Question: 249

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 proactively detect and respond to cyber threats before they cause damage
C. To perform routine maintenance on cybersecurity tools
D. To report all suspicious activities to the authorities

Answer: B

Question: 250

Why is continuous learning important for threat hunters?

A. Threat hunting techniques do not change over time.
B. Continuous learning allows threat hunters to keep up with evolving cybersecurity threats and techniques.
C. Continuous learning is not necessary for effective threat hunting.
D. Continuous learning is only relevant for junior-level threat hunters.

Answer: B

Question: 251

How can threat hunting contribute to improving an organization's overall security posture?

A. By ignoring potential threats to focus on more pressing issues
B. By proactively detecting and responding to threats before they escalate
C. By relying solely on external security measures like firewalls and antivirus software
D. By outsourcing threat hunting to third-party vendors

Answer: B

Question: 252

What is the main goal of threat hunting in cybersecurity?

A. Identifying known threats
B. Detecting all security incidents
C. Proactively seeking out potential security threats
D. Maintaining system availability

Answer: C

Question: 253

What is the purpose of threat modeling in cybersecurity?

A. Identifying vulnerabilities in a system
B. Developing software applications
C. Implementing network security protocols
D. Conducting penetration testing

Answer: A

Question: 254

Which of the following is a commonly used threat modeling approach?

A. Agile development
B. Waterfall model
C. STRIDE model
D. Scrum methodology

Answer: C

Question: 255

What does the DREAD model assess in threat modeling?

A. Impact
B. Vulnerability
C. Probability
D. All of the above

Answer: D

Question: 256

True or False: Threat modeling techniques are only relevant during the initial development phase of a project.

A. True
B. False

Answer: B

Question: 257

Which of the following is a key step in threat modeling techniques?

A. Identifying potential threats
B. Developing secure code
C. Performing vulnerability scans
D. Conducting user acceptance testing

Answer: A

Question: 258

What role does data flow diagram play in threat modeling?

A. Identifying security controls
B. Mapping the flow of data
C. Evaluating network protocols
D. Conducting penetration testing

Answer: B

Question: 259

What is Threat Actor Attribution?

A. The process of identifying the motive of threat actors
B. The process of determining the location of threat actors
C. The process of identifying and attributing cyber threats to specific individuals or groups
D. The process of blocking access to threat actors

Answer: C

Question: 260

Which of the following techniques can help in Threat Actor Attribution?

A. Geotargeting
B. Forensics analysis
C. Social media analysis
D. All of the above

Answer: D

Question: 261

What role does Threat Intelligence play in Threat Actor Attribution?

A. Threat Intelligence is not useful for Threat Actor Attribution
B. Threat Intelligence provides information and context about potential threat actors
C. Threat Intelligence can directly identify threat actors
D. Threat Intelligence only focuses on mitigation strategies

Answer: B

Question: 262

Which of the following factors can help in identifying threat actors?

A. Malware signatures
B. Tactics, Techniques, and Procedures (TTPs)
C. IP addresses
D. All of the above

Answer: D

Question: 263

What is the purpose of OSINT in Threat Actor Attribution?

A. To encrypt data
B. To gather information from public sources
C. To analyze network traffic
D. To secure cloud environments

Answer: B

Question: 264

In Threat Actor Attribution, what is a false flag operation?

A. A technique used by threat actors to avoid detection
B. A deliberate attempt by threat actors to mislead investigators by pretending to be someone else
C. A security mechanism used to block suspicious traffic
D. A type of malware used for attribution

Answer: B

Question: 265

How can Threat Actor Attribution help in cyber defense?

A. By identifying patterns of behavior and techniques used by specific threat actors
B. By providing direct access to threat actors' systems
C. By blocking all incoming network traffic
D. By monitoring employees' activities

Answer: A

Question: 266

What is the significance of attribution in cybersecurity investigations?

A. Attribution helps in determining the cost of a cyber incident
B. Attribution helps in understanding the motives and capabilities of threat actors
C. Attribution is not important in cybersecurity investigations
D. Attribution is a legal requirement

Answer: B

Question: 267

What does Behavior-based analytics focus on in Threat Actor Attribution?

A. Metadata analysis
B. Identifying known IP addresses
C. Analyzing user behavior to detect anomalous activities
D. Using encryption techniques

Answer: C

Question: 268

How can Threat Actor Attribution help in improving incident response?

A. By blocking all network traffic immediately
B. By providing information on the tools and techniques used by threat actors
C. By increasing the attack surface
D. By ignoring threat actors' activities

Answer: B

Question: 269

Which of the following is NOT a common challenge in Threat Actor Attribution?

A. False flag operations
B. Lack of skilled personnel
C. Abundance of threat intelligence
D. Limited access to relevant data

Answer: C

Question: 270

How can Threat Actor Attribution assist in developing targeted security measures?

A. By focusing on generic security measures
B. By identifying specific threat actor tactics and capabilities
C. By blocking all incoming network traffic
D. By avoiding attribution altogether

Answer: B

Question: 271

What is the purpose of using network traffic analysis as a threat hunting technique?

A. To monitor user activity on endpoints
B. To detect unusual patterns or anomalies in network traffic
C. To analyze log files for known threat signatures
D. To conduct penetration testing on the network

Answer: B

Question: 272

Which of the following is an example of a passive threat hunting technique?

A. Intrusion detection system (IDS)
B. Penetration testing
C. Event correlation
D. Packet capture analysis

Answer: D

Question: 273

How does endpoint monitoring contribute to threat hunting?

A. By analyzing network traffic
B. By identifying vulnerabilities in the network
C. By monitoring user activity on endpoints
D. By detecting malicious activities on individual devices

Answer: D

Question: 274

Which technique involves deploying a series of honey pots to lure attackers and gather information about their tactics?

A. Network traffic analysis
B. Deception technology
C. Signature-based detection
D. Threat intelligence analysis

Answer: B

Question: 275

Behavioral analysis applies machine learning algorithms to detect anomalies in what type of data?

A. Network traffic
B. Log files
C. Endpoint activity
D. Threat intelligence reports

Answer: C

Question: 276

What is the main goal of threat intelligence analysis as a threat hunting technique?

A. To monitor network traffic
B. To identify vulnerabilities
C. To gather information about potential threats
D. To conduct penetration testing

Answer: C

Question: 277

Which technique involves actively engaging with threat actors to gather information about their identities and motivations?

A. Threat intelligence analysis
B. Open-source intelligence (OSINT)
C. Threat actor engagement
D. Incident response

Answer: C

Question: 278

What is the purpose of using sandboxing as a threat hunting technique?

A. To analyze malware behavior in a controlled environment
B. To monitor network traffic
C. To conduct penetration testing
D. To analyze log files

Answer: A

Question: 279

Which technique involves monitoring user activity on endpoints to detect unusual or suspicious behavior?

A. Endpoint monitoring
B. Threat intelligence analysis
C. Behavioral analysis
D. Signature-based detection

Answer: A

Question: 280

Indicators of compromise (IOCs) are used in which threat hunting technique?

A. Network traffic analysis
B. Threat actor attribution
C. Threat modeling
D. Data exfiltration detection

Answer: A

Question: 281

Which technique involves manually reviewing log files and analyzing them for signs of malicious activity?

A. Network traffic analysis

B. Signature-based detection
C. Log file analysis
D. Incident response

Answer: C

Question: 282

What technique involves searching for patterns or behaviors indicative of potential threats in network traffic logs?

A. Packet analysis
B. DNS analysis
C. Netflow analysis
D. SIEM analysis

Answer: A

Question: 283

What is the first step in the Threat Hunting Process?

A. Analyzing existing threat intelligence
B. Identifying potential threats
C. Deploying security tools
D. Creating a threat hunting hypothesis

Answer: D

Question: 284

What is the second step in the Threat Hunting Process?

A. Analyzing existing threat intelligence
B. Identifying potential threats
C. Deploying security tools
D. Validating the hypothesis

Answer: A

Question: 285

During which step of the Threat Hunting Process do threat hunters typically use security tools like SIEMs and EDR?

A. Analyzing existing threat intelligence
B. Identifying potential threats
C. Deploying security tools

D. Validating the hypothesis

Answer: C

Question: 286

What is the final step in the Threat Hunting Process?

A. Analyzing existing threat intelligence
B. Identifying potential threats
C. Mitigating the threats
D. Documenting findings and lessons learned

Answer: D

Question: 287

What is the purpose of validating the threat hunting hypothesis in the process?

A. To confirm existing threat intelligence
B. To identify potential threats
C. To determine the effectiveness of deployed security tools
D. To test the hypothesis for accuracy

Answer: D

Question: 288

When should a threat hunting team revisit their hypothesis during the process?

A. Before analyzing existing threat intelligence
B. Before deploying security tools
C. After validating the hypothesis
D. Throughout the entire process

Answer: D

Question: 289

In the Threat Hunting Process, what step involves proactively searching for indicators of compromise (IoCs)?

A. Analyzing existing threat intelligence
B. Identifying potential threats
C. Deploying security tools
D. Threat hunting activity

Answer: D

Question: 290

During the Threat Hunting Process, why is it important to document findings and lessons learned?

A. To share with the security team
B. To report to management
C. To build threat intelligence
D. To improve future threat hunting efforts

Answer: D

Question: 291

What role do key performance indicators (KPIs) play in the Threat Hunting Process?

A. To identify potential threats
B. To measure the effectiveness of threat hunters
C. To deploy security tools
D. To analyze existing threat intelligence

Answer: B

Question: 292

How can threat hunting teams ensure they are continuously improving their process?

A. By analyzing existing threat intelligence
B. By deploying more security tools
C. By attending regular training sessions
D. By documenting findings and lessons learned

Answer: D

Question: 293

What is one benefit of a structured Threat Hunting Process?

A. It reduces the need for security tools
B. It streamlines investigation workflows
C. It eliminates the need for threat intelligence D. It increases the number of false positives

Answer: B

Question: 294

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 slow down the process
D. They only work for specific types of threats

Answer: B

Question: 295

What is the primary goal of Threat Hunting Outcomes?

A. To identify and mitigate vulnerabilities
B. To detect and respond to incidents
C. To proactively search for threats and adversaries
D. To assess the overall security posture

Answer: C

Question: 296

Which of the following is a common outcome of successful threat hunting?

A. Increased vulnerability exposure B. Reduced incident response time C. Higher false positive rate D. Decreased security awareness

Answer: B

Question: 297

In the context of Threat Hunting Outcomes, what does "TTPs" stand for?

A. Technical Threat Patterns
B. Targeted Threat Personnel
C. Tactics, Techniques, and Procedures
D. Threat Testing Protocols

Answer: C

Question: 298

Which of the following best describes the purpose of threat hunting metrics in outcomes assessment?

A. To track the number of security tools in use
B. To assess the effectiveness of security policies
C. To measure and evaluate the success of threat hunting activities
D. To identify potential threat actors

Answer: C

Question: 299

When assessing Threat Hunting Outcomes, what are some common key performance indicators (KPIs) that may be used?

A. Number of security alerts generated
B. Time to detect and respond to incidents
C. Number of system vulnerabilities identified
D. All of the above

Answer: B

Question: 300

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

Question: 301

What is the primary goal of threat hunting?

A. Identifying false positives
B. Proactively searching for threats in the network
C. Responding to security incidents
D. Patching vulnerabilities

Answer: B

Question: 302

What is the difference between proactive and reactive threat hunting?

A. Proactive threat hunting focuses on investigating known threats, while reactive threat hunting focuses on preventing future threats.
B. Proactive threat hunting focuses on preventing future threats, while reactive threat hunting focuses on investigating known threats.
C. There is no difference between proactive and reactive threat hunting.
D. Proactive threat hunting focuses on responding to security incidents, while reactive threat hunting focuses on searching for threats.

Answer: B

Question: 303

Why is threat intelligence important in threat hunting?

A. It allows threat hunters to predict future attacks before they happen.
B. It provides detailed information on potential threats and adversaries.
C. It helps in responding to security incidents.
D. It is not important in threat hunting.

Answer: B

Question: 304

What is the purpose of establishing baselines in threat hunting?

A. To determine the resources needed for threat hunting.
B. To identify deviations from normal behavior in the network.
C. To track the historical records of security incidents.
D. To prioritize security alerts.

Answer: B

Question: 305

How does threat hunting differ from traditional security monitoring?

A. Threat hunting is a reactive approach, while traditional security monitoring is proactive.
B. Threat hunting focuses on actively searching for threats, while traditional security monitoring passively looks for alerts.
C. Threat hunting relies solely on automated tools, while traditional security monitoring involves manual analysis.
D. There is no difference between threat hunting and traditional security monitoring.

Answer: B

Question: 306

What is the role of hypothesis-driven hunting in threat hunting?

A. It involves randomly searching for threats without any specific goal.
B. It focuses on forming educated guesses about potential threats and testing them through investigation.
C. It relies solely on automated tools for threat detection.
D. It is not a common practice in threat hunting.

Answer: B

Question: 307

Why is it important for organizations to have trained threat hunters?

A. Trained threat hunters can eliminate all security threats in the network.
B. They can effectively detect and respond to sophisticated threats.
C. Organizations can save costs by not investing in threat hunting training.
D. Trained threat hunters do not add value to the security posture of an organization.

Answer: B

Question: 308

What is the difference between threat hunting and incident response?

A. Threat hunting involves investigating potential threats before they manifest, while incident response focuses on reacting to security incidents after they occur.
B. Threat hunting and incident response are the same thing.
C. Threat hunting focuses on manual analysis, while incident response relies on automated tools.
D. Threat hunting only deals with low-level security incidents, while incident response tackles high- level threats.

Answer: A

Question: 309

How can threat hunting help in improving an organization's security posture?

A. By identifying and mitigating potential threats before they cause damage.
B. By solely focusing on responding to security incidents.
C. By ignoring security alerts generated by monitoring tools.
D. By conducting routine security assessments.

Answer: A

Question: 310

What is the importance of collaboration between threat hunters and other cybersecurity teams?

A. Collaboration is not important in threat hunting.
B. It can help in sharing threat intelligence and insights across different teams.
C. It can lead to conflicts within the organization.
D. It is solely the responsibility of threat hunters to manage security incidents.

Answer: B

Question: 311

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. It slows down the threat hunting process.
D. Data collection is solely the responsibility of threat hunters.

Answer: B

Question: 312

What is the difference between threat hunting and traditional security monitoring?

A. Threat hunting is focused on proactively searching for threats, while traditional security monitoring is typically reactive.
B. Traditional security monitoring relies on automated tools, while threat hunting involves a more manual and strategic approach.
C. Threat hunting is an ongoing process, while traditional security monitoring is usually event-driven.
D. Threat hunting involves generating hypotheses based on intelligence, while traditional security monitoring looks for known patterns of malicious activity.

Answer: A

Question: 313

What is the purpose of threat modeling in cybersecurity?

A. To identify potential threats and vulnerabilities in a system
B. To fix security issues after they have caused damage
C. To assess employee training programs
D. To enhance customer service

Answer: A

Question: 314

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

Question: 315

What is the goal of using data flow diagrams in threat modeling?

A. To identify potential attacks on the network infrastructure
B. To map out the flow of data in a system to identify potential vulnerabilities
C. To predict the future cyber threat landscape
D. To create a timeline of past security incidents

Answer: B

Question: 316

Which step in the threat modeling process involves considering what an attacker could do if they exploited a vulnerability?

A. Define the System
B. Identify Threats
C. Determine Vulnerabilities
D. Mitigate Risks

Answer: B

Question: 317

What is the primary focus of the STRIDE threat modeling technique?

A. Attack Trees
B. Data Flow Diagrams
C. Security design principles
D. Threat classification based on six categories

Answer: D

Question: 318

Which of the following is an example of an abuse case in threat modeling?

A. A user exploiting a vulnerability to gain unauthorized access to sensitive data
B. A software bug causing a system crash
C. Network protocols being misconfigured
D. Regular security audits performed by the IT team

Answer: A

Question: 319

What is Threat Actor Attribution?

A. The act of identifying a threat actor's motivation
B. The act of identifying a threat actor's location
C. The act of identifying a threat actor's email address
D. The act of identifying a threat actor's name

Answer: B

Question: 320

What is OSINT in the context of threat actor attribution?

A. Open Source Intelligence
B. Operating System Intelligence
C. Outbound Security Investigation
D. Open Security Incident Notification

Answer: A

Question: 321

Which of the following is not a common indicator used in threat actor attribution?

A. IP address
B. Email address
C. MAC address
E. Employee age

Answer: D

Question: 322

What is the purpose of using TTPs in threat actor attribution?

A. To identify the threat actor's Tactics, Techniques, and Procedures
B. To identify the threat actor's location
C. To identify the threat actor's email address
D. To identify the threat actor's password

Answer: A

Question: 323

Which of the following is a high-level approach to threat actor attribution?

A. Top-Down Approach
B. Bottom-Up Approach
C. Middle-Out Approach
D. Left-Right Approach

Answer: A

Question: 324

What is the significance of understanding threat actor motivation in attribution?

A. It helps in understanding their objectives and goals
B. It helps in identifying their email addresses
C. It helps in understanding their physical location
D. It helps in understanding their favorite color

Answer: A

Question: 325

Which of the following is an example of a nation-state threat actor attribution technique?

A. Using Geopolitical Context
B. Using IP Address Logs
C. Using Twitter Handles
D. Using Office Locations

Answer: A

Question: 326

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: A

Question: 327

What is a challenge often faced in threat actor attribution?

A. False Flags
B. Lack of data
C. Clear identification
D. Predicting future attacks

Answer: B

Question: 328

Which of the following is not a primary goal of threat actor attribution?

A. Identify motivations and objectives
B. Directly confront threat actors
C. Prevent future attacks
D. Share threat intelligence

Answer: B

Question: 329

How can threat actor attribution aid in threat hunting?

A. By providing insights into the threat actor's methods and behaviors
B. By identifying potential future targets
C. By launching offensive cyber operations
D. By preventing all types of cyber attacks

Answer: A

Question: 330

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: B

Question: 331

What is the primary goal of "baiting" as a threat hunting technique?

A. To lure attackers into a controlled environment
B. To actively seek out threat actors in the network
C. To analyze logs and detect anomalies
D. To perform vulnerability scans on all systems

Answer: A

Question: 332

Which of the following is a common technique used in threat hunting to track lateral movement of attackers within a network?

A. Port scanning
B. DNS tunneling
C. Log analysis
D. Privilege escalation

Answer: C

Question: 333

What is the purpose of using "sandboxing" as a threat hunting technique?

A. To isolate malicious files and observe their behavior
B. To establish secure communication channels for threat intelligence
C. To hide critical assets from potential attackers
D. To encrypt data at rest and in transit

Answer: A

Question: 334

Which threat hunting technique involves creating custom YARA rules to detect specific malware families?

A. Signature-based detection
B. Log analysis

C. Threat intelligence sharing D. Network traffic analysis

Answer: A

Question: 335

What type of analysis is performed when using "behavioral analysis" as a threat hunting technique?

A. Statistical analysis
B. Anomaly detection
C. File signature matching
D. Regular expression analysis

Answer: B

Question: 336

In the context of threat hunting, what is the purpose of conducting "incubation"

A. To slow down the attack process
B. To observe the evolution of attack tactics
C. To deploy additional security controls
D. To directly confront threat actors

Answer: B

Question: 337

Which technique involves creating "honeypots" to divert and detect potential attackers?

A. Endpoint monitoring
B. Threat intelligence analysis
C. Lateral movement tracking
D. Deception technology

Answer: D

Question: 338

What is the primary purpose of "threat hunting playbooks" in threat hunting techniques?

A. To document potential threats for future reference
B. To automate threat detection and response processes
C. To establish threat intelligence sharing frameworks
D. To guide analysts in structured investigation processes

Answer: D

Question: 339

Which technique involves analyzing network traffic patterns to identify malicious activity?

A. File integrity monitoring
B. SIEM correlation analysis
C. Network traffic analysis
D. Intrusion detection system

Answer: C

Question: 340

What technique involves simulating attack scenarios to test the effectiveness of security controls?

A. Threat modeling
B. Red teaming
C. Penetration testing
D. Endpoint monitoring

Answer: B

Question: 341

What is the main focus of "intelligence-led threat hunting" as a technique?

A. Proactive identification of unknown threats
B. Reactive analysis of historical attack data
C. Automated containment of security incidents
D. Passive monitoring of network traffic

Answer: A

Question: 342

What is the goal of using "Endpoint Analysis" as a threat hunting technique?

A. to monitor network traffic
B. to scan for vulnerabilities on network devices
C. to analyze data collected from endpoints
D. to simulate phishing attacks

Answer: C

Question: 343

What is the first step in the threat hunting process according to common methodologies?

A. Threat modeling
B. Threat actor attribution
C. Hypothesis generation
D. Data collection

Answer: C

Question: 344

During which phase of the threat hunting process would you analyze the collected data for signs of potential threats?

A. Data collection
B. Hypothesis generation
C. Investigation
D. Strategy refinement

Answer: C

Question: 345

Which step in the threat hunting process focuses on creating a plan to respond to identified threats?

A. Strategy refinement
B. Hypothesis generation
C. Investigation
D. Data collection

Answer: A

Question: 346

In the threat hunting process, what is the purpose of the data collection phase?

A. Identify potential threats Analyze collected data Develop hypotheses Refine strategies
B.
C.
D.

Answer: B

Question: 347

Which step in the threat hunting process involves continuously monitoring the environment for new threats?

A. Data collection
B. Strategy refinement
C. Investigation
D. Threat monitoring

Answer: D

Question: 348

What is the final phase in the threat hunting process where the effectiveness of the threat hunting activities is evaluated?

A. Strategy refinement
B. Investigation
C. Validation
D. Reporting

Answer: C

Question: 349

During which phase of the threat hunting process would you develop and test hypotheses based on collected data?

A. Data collection
B. Strategy refinement
C. Hypothesis generation
D. Reporting

Answer: C

Question: 350

Which step in the threat hunting process involves refining the initial plan based on feedback and experience?

A. Reporting
B. Validation
C. Strategy refinement
D. Threat monitoring

Answer: C

Question: 351

What is the primary objective of the investigation phase in the threat hunting process?

A. Validate hypotheses
B. Develop new strategies

C. Collect more data
D. Analyze collected data

Answer: D

Question: 352

Which phase of the threat hunting process involves documenting the findings and recommendations for future actions?

A. Data collection
B. Validation
C. Reporting
D. Threat monitoring

Answer: C

Question: 353

In the threat hunting process, what is the purpose of the strategy refinement phase?

A. Develop hypotheses
B. Adjust the current plan
C. Collect more data
D. Celebrate successes

Answer: B

Question: 354

What is the purpose of the investigation phase in the threat hunting process?

A. Analyzing data for potential threats
B. Creating a plan to respond to identified threats
C. Developing and testing hypotheses
D. Documenting findings and recommendations

Answer: A

Question: 355

What is the primary goal of threat hunting outcomes?

A. Increase network latency
B. Improve incident response time
C. Decrease network visibility
D. Enhance user productivity

Answer: B

Question: 356

Which of the following is NOT a common outcome of threat hunting?

A. Identification of unknown threats
B. Reduction of false positives
C. Increased performance of network devices
D. Improved security posture

Answer: C

Question: 357

In threat hunting outcomes, what does an increase in the organization's security posture mean?

A. Reduced number of security controls
B. Improved resilience to cyberattacks
C. Decreased collaboration with security teams
D. Weakened security defenses

Answer: B

Question: 358

Which of the following is a key aspect of effective threat hunting outcomes?

A. Reactive approach to incidents
B. Focus on high-traffic network areas only
C. Continuous monitoring and analysis
D. Reliance solely on automated tools

Answer: C

Question: 359

What is the importance of threat hunting outcomes in enhancing cybersecurity?

A. Decrease in threat intelligence sharing
B. Better understanding of adversaries' tactics
C. Increase in network vulnerabilities
D. Slow response to security incidents

Answer: B

Question: 360

How can threat hunting outcomes contribute to improving incident response capabilities?

A. By ignoring potential threats
B. By focusing solely on known vulnerabilities
C. By proactively hunting for threats
D. By reducing the visibility of network traffic

Answer: C