QUESTION 68
Analyzing C2 traffic data to determine the infection stage often involves looking for:

A. Periodic access to social media sites
B. Regular beaconing intervals
C. Occasional use of VPN services
D. Sporadic email checking patterns

Answer: B

QUESTION 69
Recognizing the likelihood of an attack involves understanding:

A. Current fashion trends
B. Historical attack patterns
C. Future software releases
D. Global political climates

Answer: B

QUESTION 70
To determine the stage of infection within C2 communications, one must analyze:

A. The size of email attachments
B. Traffic data patterns
C. Antivirus update logs
D. Wi-Fi connection strength

Answer: B

QUESTION 71
The effectiveness of a threat hunt can be improved by:

A. Ignoring alerts during off-hours
B. Investing in continuous training for the security team
C. Only using free or built-in tools
D. Limiting documentation to save time

Answer: B

QUESTION 72
When performing a cloud-native threat hunt, which of the following is crucial to analyze?

A. Physical network devices
B. Cloud service configuration settings
C. On-premises server logs
D. Print server logs

Answer: B

QUESTION 73
What does the Threat Hunting Maturity Model primarily assess in an organization's environment?

A. The effectiveness of firewall rules
B. The organization's capability to actively hunt threats
C. The number of security incidents per year
D. The budget allocated to the IT department

Answer: B

QUESTION 74
How does multiproduct integration enhance data visibility within a product?

A. By limiting data access to senior management
B. By accelerating data deletion processes
C. By aggregating and correlating data across platforms
D. By reducing the overall data storage needs

Answer: C

QUESTION 75
The primary use of unstructured threat hunting is to:

A. Follow a strict set of rules for analysis
B. Explore the network for anomalies without predefined hypotheses
C. Conduct compliance audits
D. Develop security policies

Answer: B

QUESTION 76
An attack's timeline can help distinguish between:

A. An insider threat and an external attacker
B. A brute force attack and a DDoS attack
C. An authorized assessment and an unauthorized attack
D. The use of AI and manual hacking techniques

Answer: C

QUESTION 77
When determining the priority of attacks based on the Cyber Kill Chain, which stage is crucial for early detection?

A. Reconnaissance
B. Weaponization

C. Installation
D. Command and Control

Answer: A

QUESTION 78
In the context of threat actor attribution, TTPs stand for:

A. Tools, Techniques, and Procedures
B. Tactics, Techniques, and Procedures
C. Targets, Tactics, and Procedures
D. Techniques, Targets, and Programs

Answer: B

QUESTION 79
Data interpreted from memory-specific tools can reveal:

A. The need for more RAM
B. Evidence of code injection attacks
C. The preferred memory brand of attackers
D. Upcoming memory sales

Answer: B

QUESTION 80
A comprehensive playbook addresses which phases of incident response? (Choose two)

A. Detection
B. Budget planning
C. Recovery
D. Lunch break scheduling

Answer: AC

QUESTION 81
Security countermeasures for identified risks might include:

A. Decreasing the complexity of passwords
B. Implementing strict access controls
C. Reducing the frequency of backups
D. Limiting the use of encryption

Answer: B

QUESTION 82
Identifying C2 communications requires analysis of:

A. Employee satisfaction surveys
B. Application, processes, and logs
C. Marketing campaign effectiveness
D. Financial transaction logs

Answer: B

QUESTION 83
For detecting memory-resident malware, it's essential to analyze:

A. Disk storage allocation
B. Memory allocation patterns
C. Cloud storage access logs
D. USB device history

Answer: B

QUESTION 84
Which scripting language is commonly used for automating the data analysis in threat hunting?

A. C++
B. Python
C. Java
D. HTML

Answer: B

QUESTION 85
What are the advantages of using automation in the operation of a SOC? (Choose two)

A. Reduces the need for human intervention
B. Increases the time to detect and respond to incidents
C. Decreases false positive rates
D. Enhances the ability to detect complex threats

Answer: AD

QUESTION 86
MITRE CAPEC is used to prioritize attacks based on:

A. The cost of potential data breaches
B. The complexity of attack patterns
C. The attacker's motivation and resources
D. The likelihood of detection

Answer: B

QUESTION 87
To detect advanced persistent threat actors, analysts must look for artifacts related to:

A. Only the initial infection vector
B. Broad patterns of normal user behavior
C. Deep and complex interrelations of TTPs
D. Generic signatures of common malware

Answer: C

QUESTION 88
The use of MITRE CAPEC helps in:

A. Designing user interfaces
B. Modeling common attack patterns for software
C. Managing HR processes
D. Optimizing network traffic

Answer: B

QUESTION 89
The payload of a cyber attack refers to:

A. The method used to deliver a cyber attack
B. The software or data that is intended to exploit a vulnerability
C. The document that outlines the attacker's motives
D. The timeline of the attack from start to finish

Answer: B

QUESTION 90
Detection tools are limited in their effectiveness due to: (Choose two)

A. The dynamic nature of cyber threats
B. The physical security of the data center
C. Encryption used by network protocols
D. The evolving tactics of threat actors

Answer: AD

QUESTION 91
When recommending changes to improve threat hunting outcomes, it's important to consider:

A. The potential impact on IT workload and resources
B. The preferences of external auditors
C. The latest cybersecurity fads
D. Reducing the scope of the hunt to minimize effort

Answer: A

QUESTION 92
Reverse engineering malware helps in understanding its:

A. Color scheme
B. Purpose and functionality
C. Creator's favorite programming language
D. Copyright date

Answer: B

QUESTION 93
Known gaps in detection can include: (Choose two)

A. Unpatched vulnerabilities
B. Fully updated software
C. Misconfigured firewalls
D. Strong password policies

Answer: AC

QUESTION 94
Which level of the Pyramid of Pain is most difficult for attackers to change and adapt to when detected?

A. Hash values
B. IP addresses

C. Domain names
D. TTPs (Tactics, Techniques, and Procedures)

Answer: D

QUESTION 95
The PASTA method is used to:

A. Prioritize assets based on their criticality
B. Prepare Italian dishes in the company cafeteria
C. Perform automated static analysis on software
D. Conduct penetration testing on network infrastructure

Answer: A

QUESTION 96
An augmentation of the detection methodology may necessitate:

A. Decreasing the variety of data sources monitored
B. Implementing a zero-trust architecture
C. Relying more heavily on predefined threat signatures
D. Discouraging proactive threat research

Answer: B

QUESTION 97
When interpreting the tactics, techniques, and procedures of a threat actor, which of the following is most crucial?

A. The volume of data exfiltrated
B. The specific malware variant used
C. The pattern of lateral movement within the network
D. The time of day the attack occurred

Answer: C

QUESTION 98
Which tool is specifically designed for static analysis of executable files for vulnerabilities?

A. PE Checker
B. OWASP ZAP
C. BURP Suite
D. Metasploit

Answer: A

QUESTION 99
What does the term "honeypot" refer to in threat hunting techniques?

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

Answer: A

QUESTION 100
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 101
In the context of the threat hunting process, what does the term "pivot" mean?

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

Answer: C

QUESTION 102
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: B

QUESTION 103
How can threat hunting help improve an organization's overall security posture?

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

Answer: D

QUESTION 104
Which of the following best describes an advanced persistent threat (APT)?

A. A short-term financial fraud scheme
B. A quickly evolving malware variant
C. A long-term, targeted attack campaign
D. An opportunistic ransomware attack

Answer: C

QUESTION 105
Blocking C2 traffic effectively requires:

A. Ignoring encrypted traffic as it's secure by default
B. Focusing on inbound traffic only
C. Analyzing network traffic for anomalies
D. Assuming all internal network traffic is safe

Answer: C

QUESTION 106
When selecting indicators for attribution, which of the following is considered a weak indicator on its own?

A. A unique tool or piece of malware
B. Time of attack
C. Specificity of the target
D. Language of the attack code

Answer: B

QUESTION 107
Analytical gaps in threat hunting methodologies can result in:

A. An overreliance on automated alerting systems
B. Perfect detection with no false negatives
C. Improved threat actor attribution
D. Missed detection opportunities

Answer: D

QUESTION 108
Diagnosing analytical gaps is crucial for:

A. Justifying the reduction of the cybersecurity budget
B. Identifying underutilized resources
C. Ignoring emerging threat vectors
D. Complying with outdated regulations

Answer: B

QUESTION 109
The MITRE CAPEC database is best used for understanding:

A. Compliance requirements
B. Common attack patterns
C. Encryption standards
D. Firewall configurations

Answer: B

QUESTION 110
Memory-resident attacks can be analyzed using which tool?

A. Wireshark
B. Nessus
C. Volatility
D. Nmap

Answer: C

QUESTION 111
What is the primary goal of threat hunting?

A. To create legal reports for compliance
B. To prevent users from accessing malicious websites

C. To proactively find and mitigate potential threats before they cause harm
D. To install antivirus software on all endpoints

Answer: C

QUESTION 112
Selecting the delivery method for an attack, which aspect is least likely to be used by a legitimate penetration tester without explicit authorization?

A. Social engineering employees over email
B. Deploying a backdoor for later access
C. Performing vulnerability scanning
D. Testing physical security measures

Answer: B

QUESTION 113
Constructing a signature for detection involves:

A. Identifying unique patterns of attack
B. Estimating the cost of an attack
C. Predicting future attack vectors
D. Calculating the downtime caused by an attack

Answer: A

QUESTION 114
Security countermeasures for mitigating identified risks include:

A. Disabling all firewall rules to prevent false positives
B. Encrypting sensitive data both at rest and in transit
C. Reducing the complexity of network passwords
D. Decreasing the frequency of security audits

Answer: B

QUESTION 115
What artifact would be considered at the top of the Pyramid of Pain and indicates a high level of sophistication in modifying behaviors to avoid detection?

A. MD5 hashes
B. IP addresses
C. TTPs
D. Domain names

Answer: C

QUESTION 116
Python scripts in threat hunting are used for:

A. Designing corporate websites
B. Automating detection and analysis tasks
C. Managing employee records
D. Conducting online marketing campaigns

Answer: B

QUESTION 117
Which of the following indicates an authorized assessment rather than an attack?

A. Use of a known exploit tool
B. Presence of a payload that encrypts data for ransom
C. A detailed report provided at the end of the activities
D. Quick escalation of privileges upon entry

Answer: C

QUESTION 118
The effectiveness of threat modeling techniques is enhanced by:

A. Limiting access to threat intelligence
B. Integrating diverse data sources for a comprehensive view
C. Focusing solely on internal threats
D. Using a single threat intelligence source

Answer: B

QUESTION 119
The priority level of attacks based on the MITRE CAPEC model focuses on the:

A. Age of the technology used
B. Type of data at risk
C. Attack pattern's complexity and risk
D. Geographic location of the attacker

Answer: C

QUESTION 120
Identifying a threat actor's tactics involves understanding their:

A. Preferred malware encryption algorithm
B. Overall objectives and goals
C. Choice of programming language
D. Specific vulnerabilities targeted

Answer: B

QUESTION 121
The process of removing outdated threat intelligence involves:

A. Updating firewall rules
B. Retraining machine learning models
C. Reviewing and discarding no longer relevant data
D. Patching software vulnerabilities

Answer: C