Get Free Cisco 300-220 Dumps PDF Questions

Why risk failure? Download updated Cisco Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps exam PDF questions today. Practice with real 300-220 dumps and verified answers designed to help you ace your certification quickly using PrepBolt 300-220 exam pdf questions and answers.

Thank you for Downloading 300-220 exam PDF Demo

https://prepbolt.com/300-220.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

A SOC repeatedly discovers similar attacker behaviors during separate hunts, indicating recurring detection gaps. What process change MOST effectively prevents rediscovery of the same threats?

Options:

A- Increasing analyst staffing
B- Automating hunt execution
C- Converting hunt findings into permanent detections
D- Conducting more frequent unstructured hunts

Answer:

C

Explanation:

The correct answer is converting hunt findings into permanent detections. Threat hunting is only effective when discoveries are operationalized.

Without converting findings into SIEM, EDR, or NDR detections, organizations repeatedly identify the same attacker behaviors, wasting time and resources. Options A, B, and D improve capacity but do not eliminate blind spots.

Mature threat hunting programs ensure that:

Hunts produce detection rules

Alerts are tuned and validated

Knowledge is institutionalized

This is a defining trait of high-maturity security organizations and directly improves resilience. Therefore, option C is correct.

Question 2

Question Type: MultipleChoice

A threat hunter wants to detect credential dumping attempts that bypass traditional malware detection. Which telemetry source is MOST effective for this purpose?

Options:

A- Email gateway attachment logs
B- Endpoint memory access telemetry
C- DNS query logs
D- Firewall allow/deny logs

Answer:

B

Explanation:

The correct answer is endpoint memory access telemetry. Credential dumping often involves accessing sensitive memory regions, such as LSASS, rather than deploying obvious malware.

Modern attackers frequently use:

Legitimate tools

In-memory techniques

Living-off-the-land binaries

These methods bypass file-based detection entirely. Email, DNS, and firewall logs provide limited visibility into memory-level abuse.

Endpoint memory telemetry enables detection of:

Unauthorized LSASS access

Suspicious handle requests

Abnormal process injection

This telemetry is foundational for detecting credential access techniques in modern environments. Therefore, option B is correct.

Question 3

Question Type: MultipleChoice

During multiple intrusions, analysts observe that attackers consistently perform internal reconnaissance before privilege escalation, avoid noisy exploitation, and limit actions to business hours of the victim's region. Why is this observation important for attribution?

Options:

A- It confirms the use of a specific exploit kit
B- It indicates an advanced persistence mechanism
C- It reveals operational discipline and intent
D- It identifies the malware command-and-control protocol

Answer:

C

Explanation:

The correct answer is it reveals operational discipline and intent. Attribution relies heavily on understanding how attackers think and operate, not just the tools they use.

Operational discipline---such as careful reconnaissance, avoiding noisy exploitation, and operating during business hours---is a human behavioral pattern. These patterns are far more stable than infrastructure or malware and often correlate strongly with specific threat actor groups.

Option A and D focus on tooling, which changes frequently. Option B relates to persistence, not attribution.

Threat intelligence professionals use operational characteristics to distinguish between opportunistic criminals and advanced adversaries. Business-hour activity, careful lateral movement, and deliberate escalation often indicate targeted intrusions, espionage, or financially motivated but sophisticated actors.

This information helps analysts align observed behavior with known threat actor profiles, improving attribution confidence. Thus, option C is correct.

Question 4

Question Type: MultipleChoice

A security team is performing threat modeling for a hybrid environment consisting of on-prem Active Directory and Azure AD. The team wants to identify how an attacker could move from a compromised cloud identity to full on-prem domain dominance. Which modeling focus is MOST appropriate?

Options:

A- Enumerating CVEs affecting domain controllers
B- Mapping trust relationships between identity systems
C- Assigning CVSS scores to authentication mechanisms
D- Conducting packet-level network flow analysis

Answer:

B

Explanation:

The correct answer is mapping trust relationships between identity systems. Hybrid identity environments introduce complex trust boundaries that attackers routinely exploit.

Modern breaches increasingly involve identity pivoting, where attackers compromise a cloud identity and abuse synchronization, federation, or conditional access misconfigurations to escalate into on-prem Active Directory. These attack paths often do not rely on software vulnerabilities at all.

Option A is too narrow and focuses only on technical exploits. Option C measures severity but does not model movement. Option D analyzes traffic but does not explain privilege escalation pathways.

By mapping trust relationships---such as Azure AD Connect synchronization, service principals, hybrid admin roles, and conditional access exclusions---defenders can identify chained attack paths that enable privilege escalation without exploiting code.

From a threat hunting standpoint, this modeling enables:

Hypothesis-driven hunts

Detection of abnormal role assumptions

Visibility into identity abuse

This approach aligns with attack path modeling, a critical evolution of traditional threat modeling for identity-centric environments. Therefore, option B is correct.

Question 5

Question Type: MultipleChoice

A mature SOC notices that several incidents over the past year involved attackers abusing legitimate administrative tools rather than deploying custom malware. Leadership asks the threat hunting team

to improve detection coverage in a way that increases attacker cost rather than relying on easily replaceable indicators. Which detection strategy best aligns with this objective?

Options:

A- Blocking known malicious file hashes at the endpoint
B- Correlating attacker behavior across multiple MITRE ATT&CK techniques
C- Ingesting additional commercial threat intelligence feeds
D- Creating alerts for newly registered domains

Answer:

B

Explanation:

The correct answer is correlating attacker behavior across multiple MITRE ATT&CK techniques. This approach focuses on behavioral detection, which is the cornerstone of effective threat hunting and advanced security operations.

Attackers who abuse legitimate administrative tools---often referred to as living-off-the-land techniques---intentionally avoid malware-based detections. File hashes, signatures, and known indicators provide minimal value because there may be no malicious files at all. Options A and D sit at the lowest levels of the Pyramid of Pain, making them easy for adversaries to evade.

By correlating behavior across multiple ATT&CK techniques---such as credential access, lateral movement, privilege escalation, and command execution---defenders detect how the attacker operates rather than what tools they use. This forces adversaries to fundamentally change tradecraft, which is costly, risky, and time-consuming.

Option C improves visibility but does not inherently raise attacker cost. Threat intelligence feeds are reactive and often lag behind active campaigns.

From a professional threat hunting perspective, correlating multiple low-signal behaviors into a high-confidence attack pattern is how mature SOCs detect stealthy intrusions. This method also supports scalable detection engineering, improved alert fidelity, and reduced false positives.

This strategy directly aligns with higher tiers of the Threat Hunting Maturity Model and the top of the Pyramid of Pain, making option B the correct answer.

Question 6

Question Type: MultipleChoice

A threat hunting team wants to ensure hunts are repeatable, scalable, and less dependent on individual analyst intuition. What is the MOST important process improvement?

Options:

A- Increasing the number of threat intelligence feeds
B- Automating alert triage workflows
C- Standardizing hunt documentation and hypotheses
D- Blocking all suspicious activity automatically

Answer:

C

Explanation:

The correct answer is standardizing hunt documentation and hypotheses. Mature threat hunting programs move beyond ad-hoc, intuition-driven efforts.

Standardization enables:

Knowledge sharing

Consistent methodology

Repeatable hunts

Easier onboarding of new analysts

Option A and B support operations but do not improve hunting maturity. Option D is unrealistic and risky.

By documenting hypotheses, data sources, queries, findings, and outcomes, organizations institutionalize knowledge and continuously improve detection capabilities.

This is a defining characteristic of high-maturity threat hunting programs.

Therefore, option C is correct.

Thank You for trying 300-220 PDF Demo

To try our 300-220 practice exam software visit link below

https://prepbolt.com/300-220.html

Start Your 300-220 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your 300-220 preparation with actual exam questions.