DUMPSBOSS.

Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Cisco 300-220

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Threat Hunting Fundamentals	40
Topic 2, Threat Hunting Techniques	23
Topic 3, Threat Hunting with Cisco Technologies	16
Total	79

QUESTION NO: 1

The SOC team receives an alert about a user sign-in from an unusual country. After investigating the SIEM logs, the team confirms the user never signed in from that country. The incident is reported to the IT administrator who resets the user's password. Which threat hunting phase was initially used?

A. Collect and process intelligence and data

B. Response and resolution

C. Hypothesis

D. Post-incident review

ANSWER: A

Explanation:

Collect and process intelligence and data is the correct answer because the team's initial hunting activity is to use available security telemetry to establish whether the alert represents a real anomaly. The unusual-country sign-in alert provides an investigative lead, and the analysts then query and correlate SIEM authentication records, historical sign-in behavior, and geographic context. This collection and processing of identity-related evidence lets the SOC determine that the observed location is inconsistent with the user's established activity and should be treated as a likely account-compromise event.

Threat hunting depends on usable, appropriately scoped telemetry: identity-provider sign-in events, VPN records, endpoint data, DNS activity, and other logs must be collected, normalized, retained, and made searchable before analysts can validate suspicious behavior. Cisco describes threat hunting as proactively using security data and threat intelligence to identify malicious activity that automated detections may not fully resolve. In this case, examining SIEM records is the essential first action that converts an alert into evidence-based confirmation. Cisco's overview of threat hunting is available at Cisco: What Is Threat Hunting?. The importance of analyzing relevant event data during security incident handling is also reflected in NIST SP 800-61 Rev. 2.

QUESTION NO: 2

A threat hunter is investigating suspected lateral movement through Windows Management Instrumentation. The organization permits limited WMI use by approved management servers. Which two telemetry sources should be correlated to distinguish suspicious remote WMI execution from normal administration? (Choose two.)

A. Windows process-creation telemetry

B. Authentication and remote logon events

C. DNS resolver query logs

D. Email delivery records

E. Web application access logs

ANSWER: A B

Explanation:

Windows process-creation telemetry can reveal suspicious processes spawned by WMI, including unusual command lines and parent-child relationships involving WMI provider processes. Authentication and remote logon events identify the account, source system, destination system, and timing associated with the remote access.

Correlating execution evidence with authentication context allows the hunter to compare the activity against approved management servers and authorized administrative accounts. DNS logs and email delivery records do not establish whether remote WMI execution occurred.

QUESTION NO: 3

A SOC team using Cisco security technologies wants to improve its ability to detect threats that bypass traditional security controls by abusing valid user credentials. Which hunting focus MOST effectively addresses this challenge?

A. Monitoring antivirus alerts for malware detections

B. Tracking file hash reputation from threat intelligence feeds

C. Analyzing authentication behavior anomalies across users and devices

D. Blocking newly registered domains at the firewall

ANSWER: C

Explanation:

Analyzing authentication behavior anomalies across users and devices is the most effective hunting focus because attacks that use valid credentials frequently appear legitimate to controls designed to identify known malware, malicious files, or clearly suspicious destinations. Threat hunters should instead establish a baseline for normal identity activity and investigate deviations, such as unusual login times, impossible travel, authentication from unfamiliar devices or networks, abnormal access to systems, repeated failed logins followed by success, and unexpected privilege use. Correlating authentication records with endpoint, network, VPN, DNS, and identity-context telemetry helps reveal whether an apparently valid session is consistent with the user's normal behavior and authorized access patterns. This approach supports detection of compromised accounts, credential theft, lateral movement, and misuse of privileged identities before a conventional signature-based alert necessarily occurs. Cisco security architectures can provide the required identity, endpoint, and network visibility for this correlation, while Cisco Secure Network Analytics helps identify anomalous behavior across the network. Cisco describes its network analytics capabilities at Cisco Secure Network Analytics, and identity context and policy capabilities are detailed at Cisco Identity Services Engine.

QUESTION NO: 4

A threat hunter uses**Cisco Secure Endpoint**to investigate a suspected credential-harvesting attack that does not involve dropping files to disk. Which capability is MOST critical for detecting this activity?

A. File hash reputation scoring

B. Endpoint process ancestry tracking

C. Email attachment sandboxing

D. URL category filtering

ANSWER: B

Explanation:

Endpoint process ancestry tracking is most critical because fileless credential-harvesting activity is identified primarily through endpoint behavioral telemetry rather than through an on-disk artifact. Attackers commonly abuse legitimate applications and interpreters, such as Office applications, PowerShell, Windows Script Host, rundll32, or browser processes, to execute code in memory and access credentials. Investigators therefore need to determine not only that a process ran, but also which parent launched it, the command line used, the user and endpoint context, and the subsequent processes and network activity it initiated.

Cisco Secure Endpoint provides endpoint visibility through its Device Trajectory capability, which enables analysts to trace execution activity and investigate relationships among processes, files, and network connections on an affected device. This allows a hunter to recognize suspicious execution chains, including an application launching an unexpected scripting engine or a trusted system utility being used with unusual arguments. Those relationships remain useful even when malware never writes a conventional executable to disk, making process lineage essential to investigating living-off-the-land and memory-resident behavior. Cisco describes Secure Endpoint investigation and trajectory capabilities at Cisco Secure Endpoint, and Cisco's guidance on endpoint detection and response is available at Cisco Endpoint Security.

QUESTION NO: 5

A threat hunter is performing a structured hunt using **Cisco Secure Endpoint (AMP)** telemetry to identify credential harvesting activity. Which data source is MOST critical during the **data collection and processing phase** of the hunt?

A. File reputation scores from Talos

B. Endpoint process execution and memory access events

C. Threat intelligence reports from external vendors

D. User-reported suspicious activity

ANSWER: B

Explanation:

Endpoint process execution and memory access events are the most critical data source because credential harvesting is fundamentally a host-level behavioral activity. A structured hunt needs telemetry that shows which process executed, its command line and parent-child lineage, its security context, and interactions that indicate access to credential material. This evidence lets the hunter test a specific hypothesis, correlate activity over time, and distinguish ordinary administrative behavior from suspicious execution patterns.

Cisco Secure Endpoint is designed to provide endpoint detection and response visibility, including process-centric event data and activity relationships that support investigation of potentially malicious behavior. Process and memory-related telemetry is especially valuable when credential-access behavior is performed through native utilities, injected code, or other in-memory techniques that may not produce a conventional malicious-file artifact. The hunter can use this telemetry to reconstruct the execution chain, identify the affected endpoint and user context, and pivot into related activity for validation.

This also maps directly to the MITRE ATT&CK OS Credential Dumping technique, which covers attempts to obtain credentials from operating-system sources such as LSASS. Cisco Secure Endpoint capabilities are described at Cisco Secure Endpoint, and the relevant credential-access technique is documented by MITRE ATT&CK: OS Credential Dumping.

QUESTION NO: 6

A threat hunter is investigating suspected data exfiltration from an engineering workstation. The attacker is believed to be staging files locally before sending them through an approved web service. Which two endpoint behaviors are the strongest indicators of data staging? (Choose two.)

A. Creation of a large archive in a temporary directory

B. Modification of a single document in its normal project folder

C. Installation of scheduled operating-system updates

D. Browser cache writes after ordinary web browsing

E. Rapid collection of files into a newly created local directory

ANSWER: A E

Explanation:

Creation of a large archive in a user-writable or temporary location is a strong staging signal because adversaries frequently compress collected files before transfer. A process that rapidly reads files from multiple engineering repositories and writes them into a single new directory or archive also indicates aggregation of data for a later exfiltration step.

A normal document edit, a scheduled operating-system update, or a browser cache write does not by itself establish that sensitive material is being collected and prepared for transfer. The selected behaviors should be correlated with the responsible process, user context, and subsequent outbound network activity.

QUESTION NO: 7

A security team wants to create a plan to protect companies from lateral movement attacks. The team already implemented detection alerts for pass-the-hash and pass-the-ticket techniques. Which two components must be monitored to hunt for lateral movement attacks on endpoints? (Choose two.)

A. Use of the runas command

B. Linux file systems for files that have the setuid/setgid bit set

C. Use of Windows Remote Management

D. Creation of scheduled task events

E. Use of tools and commands to connect to remote shares

ANSWER: C E

Explanation:

Monitoring **Use of Windows Remote Management** provides visibility into a commonly abused remote-services channel. WinRM enables remote PowerShell and management activity using authenticated credentials; consequently, threat hunters should baseline approved administrative sources and accounts, then investigate unusual remote sessions, unexpected parent processes, abnormal command execution, and connections to multiple endpoints. This is especially important after pass-the-hash or pass-the-ticket activity because an attacker may use the acquired authentication material to access another system without needing the user's plaintext password. MITRE ATT&CK identifies Windows Remote Management as a protocol that can be used under the Remote Services lateral-movement technique. See MITRE ATT&CK: Remote Services.

Monitoring **Use of tools and commands to connect to remote shares** is also essential because SMB shares, including administrative shares, are frequently used to access remote systems, copy payloads, stage tools, and support subsequent remote execution. Endpoint telemetry should capture share connections, authentication context, process execution for share-access utilities, accessed paths, and file-write activity to administrative shares. Correlating this activity with unusual credential use and rapid connections across hosts helps expose a lateral-movement sequence rather than treating each event in isolation. MITRE documents SMB/Windows Admin Shares as a relevant remote-services mechanism for lateral movement at MITRE ATT&CK: SMB/Windows Admin Shares.