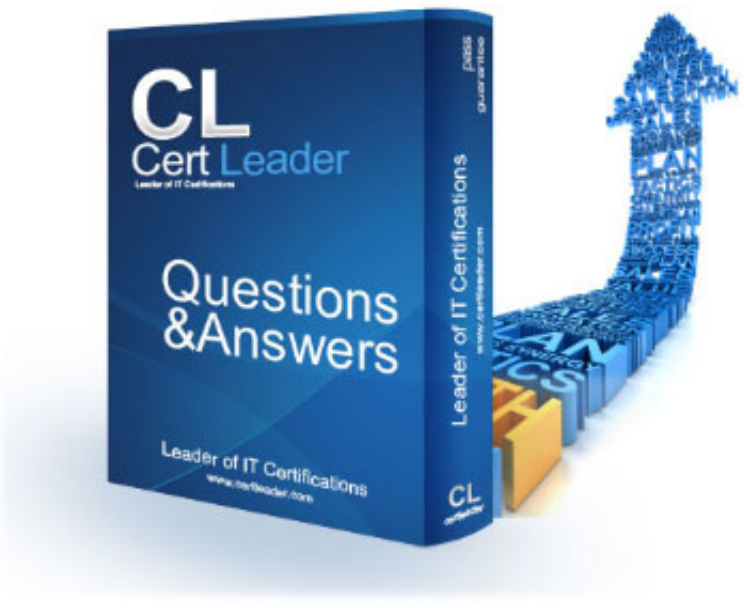
# SecOps-Pro Dumps

# Palo Alto Networks Security Operations Professional

## https://www.certleader.com/SecOps-Pro-dumps.html



**NEW QUESTION 1**
In the MITRE ATT&CK framework, which term describes the specific high-level "Why" or goal of an attacker, such as "Initial Access" or "Exfiltration"?

A. Technique
B. Tactic
C. Procedure
D. Mitigation

**Answer:** B

**Explanation:**
TheMITRE ATT&CKframework is categorized into a hierarchy that helps SOC analysts understand attacker behavior:
Tactic (B):This is theobjective/goalof the attacker. There are currently 14 tactics in the Enterprise matrix, including Reconnaissance, Persistence, and Lateral Movement. It answers the question "What is the attacker trying to achieve?"
Technique (A):This is the "How"—the specific method used to achieve a tactic (e.g., "Spearphishing Attachment" to achieve "Initial Access").
Procedure (C):The specific implementation or "recipe" used by a particular threat actor (e.g., "APT28 used a specific PowerShell script to bypass AMSI").
Mapping:Cortex XDR and XSIAM natively map alerts to these Tactics and Techniques to help analysts quickly understand the stage and intent of an attack.

**NEW QUESTION 2**
What is a primary responsibility of an incident responder in a SOC?

A. Mitigating incidents that have been escalated
B. Supervising vulnerability assessments and penetration tests
C. Determining or adjusting criticality of alerts
D. Developing incident recovery crises communications plans

**Answer:** A

**NEW QUESTION 3**
Which two types of tasks are supported in Cortex XSIAM playbooks? (Choose two.)

A. Sub-playbook
B. Script creation
C. Conditional
D. Data collection

**Answer:** AC

**NEW QUESTION 4**
Which dashboard or module in Cortex XSIAM provides visibility into unmanaged devices, unauthorized shadow IT, and cloud assets that do not currently have a Cortex agent installed?

A. Host Insights
B. Asset Inventory
C. Cloud Discovery & Exposure
D. Identity Analytics

**Answer:** C

**NEW QUESTION 5**
A customer is investigating a security incident in which unusual network traffic is observed and a malicious process is identified on an endpoint. Which Cortex XDR capability assists with correlating firewall network logs and endpoint data in this environment?

A. Log stitching
B. User authentication management
C. Indicator of compromise (IOC) rule
D. Analytics

**Answer:** A

**Explanation:**
In the Palo Alto Networks Cortex XDR ecosystem,Log Stitchingis the fundamental technology that enables the "X" (Extended) in XDR. It is the process of automatically reassembling fragmented data from disparate sources—such as Next-Generation Firewalls (NGFW), GlobalProtect, and the Cortex XDR agent—into a single, cohesive narrative.
How it Works:When a firewall identifies a network flow and an endpoint agent identifies a process execution, these are initially two separate logs. Cortex XDR uses "stitching" to link these logs by matching common attributes (such as timestamps, source/destination IP addresses, and ports) to identify theCausality Group Owner (CGO).
The Result:This allows an analyst to see exactly which local process on the endpoint (e.g., powershell.exe) was responsible for generating the specific malicious network traffic caught by the firewall. Without log stitching, these would remain two isolated events, making it much harder to prove the "cause and effect" of an attack.
Why other options are incorrect:
User authentication management:Focuses on identity and access, not the correlation of network and process telemetry.
Indicator of compromise (IOC) rule:These are typically used to flag known malicious artifacts (like a specific file hash or IP address) but do not perform the structural correlation of different log types.
Analytics:While Analyticsusesthe data provided by log stitching to identify behavioral anomalies, the specific capability that performs the correlation and "linking" of the firewall and endpoint logs is the stitching process itself.

**NEW QUESTION 6**
What is the Cortex XSOAR Marketplace?

A. Searchable collection of third-party playbooks and data models
B. Development environment for creating and sharing third-party integrations
C. Digital storefront where Cortex XSOAR training credits can be purchased and used
D. Built-in repository of installable content, including integrations and automations

**Answer:** D

**NEW QUESTION 7**
Which incident should a responder prioritize based on overall functional and informational impact to the company?

A. A user in the accounting department receives a pop-up message after visiting a website.
B. A public-facing web server has multiple failed login attempts over a short period of time.
C. An external-facing company website is currently unavailable.
D. A large upload of user data from an internal file server to a public website occurs.

**Answer:** D

**NEW QUESTION 8**
Which process in Cortex XSIAM ensures that raw logs from different vendors (e.g., Check Point, Cisco, and Microsoft) are converted into a standardized format for unified analysis?

A. Data Stitching
B. XDM Mapping
C. Entity Profiling
D. Log Ingestion

**Answer:** B

**Explanation:**
TheXDM (Cortex Data Model)is the backbone of Cortex XSIAM's ability to act as a unified SOC platform.
Standardization:Raw logs come in many formats (Syslog, JSON, LEEF).XDM Mappingis the process of taking those raw fields and "mapping" them to a common schema. For example, "src_ip," "source_address," and "sIP" from different vendors are all mapped to a single XDM field called xdm.source.ipv4.
Cross-Vendor Correlation:Once data is mapped to XDM, an analyst can write one XQL query that searches across logs fromallvendors simultaneously, which is essential for effective threat hunting in a multi-vendor environment.

**NEW QUESTION 9**
Which two functions are allowed when stitching logs in Cortex XDR? (Choose two.)

A. Providing real-time threat prevention or remediation of threats
B. Creating granular BIOC and correlation rules
C. Enabling creation of custom scripts for remediation of security incidents
D. Running investigation queries based on combined network and endpoint events

**Answer:** BD

**NEW QUESTION 10**
In Cortex XSOAR, what happens by default to an indicator (such as a malicious IP) once it reaches its configured expiration date?

A. It is permanently deleted from the XSOAR database.
B. It is moved to the "Archive" tab and cannot be used in playbooks.
C. It remains in the system but is marked as "Expired" and no longer actively pushed to integrations.
D. Its verdict is automatically changed from "Malicious" to "Benign".

**Answer:** C

**NEW QUESTION 10**
Which protocol is commonly used by Cortex XSOAR to automatically pull threat intelligence indicators from external TAXII servers?

A. STIX
B. HTTPS
C. TAXII
D. FTP

**Answer:** C

**NEW QUESTION 15**
Which metric is used by SOC management to measure the average "Dwell Time"—the duration between a successful compromise and the moment it is first identified by a security tool or analyst?

A. MTTR (Mean Time to Respond)
B. MTTA (Mean Time to Acknowledge)
C. MTTD (Mean Time to Detect)
D. MTTC (Mean Time to Contain)

**Answer:** C

**NEW QUESTION 17**
Where in Cortex XSOAR are analysts able to collaborate and converse with others for joint real-time investigations?

A. Investigations tab
B. War Room
C. Evidence Board
D. Work plan

**Answer:** B

**Explanation:**
TheWar Roomis the central collaborative feature of Cortex XSOAR. It is designed to mimic a physical "war room" where security experts gather to solve a crisis.
Real-Time Collaboration:It features a chat-like interface where analysts can post notes, upload files, and tag other team members to collaborate on a specific incident in real-time.
Shared CLI:Every analyst in the War Room sees the commands being run by others and the results of those commands. This prevents duplication of effort and ensures everyone has the same context.
Note on Evidence Board (C):While the Evidence Board displays captured artifacts, theconversation and collaborationhappen exclusively within the War Room interface.
Correction:Corrected "analystsle" to "analysts are able."

**NEW QUESTION 19**
Which component of Cortex XDR is designed to detect insider threats?

A. Forensics
B. Identity Analytics
C. Cloud Identity Engine
D. Host Insights

**Answer:** B

**Explanation:**
Identity Analytics(formerly part of the Magnifier module) is specifically designed to identify stealthy attacks that traditional signature-based tools miss, such asinsider threats, credential theft, and lateral movement.
Behavioral Baselining:It uses Machine Learning to create a "baseline" of normal behavior for every user and entity in the network. It tracks who they usually communicate with, what time they log in, and what resources they typically access.
Anomaly Detection:If a user suddenly begins accessing sensitive servers they??ve never touched before or starts transferring large amounts of data to an unusual external IP, Identity Analytics flags this as a "User Behavioral Analytics" (UBA) alert.
Focus on Identity:Unlike Host Insights (which looks at vulnerabilities) or Forensics (which looks at disk artifacts), Identity Analytics focuses purely on theactions of the user accountto find malicious intent.

**NEW QUESTION 20**
What is the WildFire verdict on a sample that does not pose a direct security threat, but is shown to display obtrusive behavior?

A. Grayware
B. Unknown
C. Benign
D. Malware

**Answer:** A

**NEW QUESTION 24**
What are the primary functions of the Causality Analysis Engine in Cortex XDR?

A. To identify the root cause of alerts and provide a complete forensic timeline of events
B. To prioritize critical alerts and reduce the overall number of alerts generated
C. To perform regular system backups and restore operations in case of failure
D. To determine only the root cause of an attack and automatically remediate threats

**Answer:** A

**NEW QUESTION 27**
What can be used to triage and determine if an artifact in Cortex XDR is malicious?
(Choose one answer)

A. Alert severity
B. MITRE tactic
C. SmartScore
D. WildFire report

**Answer:** D

**NEW QUESTION 29**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your SecOps-Pro Exam with Our Prep Materials Via below:

https://www.certleader.com/SecOps-Pro-dumps.html