

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

<https://www.2passeasy.com/dumps/SecOps-Pro/>



NEW QUESTION 1

Which statement explains the difference between the Cortex Identity Threat Detection and Response (ITDR) module and Identity Analytics in Cortex XSIAM?

- A. Identity Analytics detects suspicious logins and MFA spamming, whereas the ITDR module defends against anomalous insider activity and exfiltration to physical devices.
- B. The ITDR module is designed for compliance reporting, while Identity Analytics focuses on detecting and responding to brute force attacks and excessive logins.
- C. Identity Analytics provides prevention of suspicious logins, whereas the ITDR module focuses on advanced threat vectors.
- D. The ITDR module provides basic security event monitoring, while Identity Analytics focuses on integrating various security tools.

Answer: A

NEW QUESTION 2

An administrator needs to prevent users from connecting unauthorized USB flash drives to their corporate workstations to reduce the risk of data exfiltration. Which Cortex XDR feature should be configured?

- A. Device Control
- B. Host Insights
- C. Behavioral Threat Protection
- D. Malware Profile

Answer: A

NEW QUESTION 3

According to the Traffic Light Protocol (TLP) 2.0 standard, which classification is used for information that is restricted to the specific individuals involved in an investigation and cannot be shared further?

- A. TLP:CLEAR
- B. TLP:GREEN
- C. TLP:AMBER
- D. TLP:RED

Answer: D

NEW QUESTION 4

An analyst identifies that a custom internal application is being incorrectly flagged as malicious by the Behavioral Threat Protection (BTP) module. What is the best way to stop these alerts while maintaining security for other applications?

- A. Disable the BTP module in the endpoint's Malware Profile.
- B. Add the application's file hash to the Global Block List.
- C. Create a specific Exception for the alert from the Incident View.
- D. Move the endpoint to a policy group with no security profiles.

Answer: C

Explanation:

In Cortex XDR, Exceptions are the preferred method for tuning the platform to reduce false positives without creating broad security gaps.

Granular Control: When you create an exception from a specific alert, Cortex XDR allows you to define the scope based on specific attributes like the process name, command line, or file path.

Targeted Tuning: Unlike disabling an entire module (Option A), an exception only ignores the specific behavior for that specific application.

Ease of Use: This can be done directly from the "Check Action" or "Alerts" tab within an incident, allowing the analyst to quickly suppress future occurrences of that specific false positive.

NEW QUESTION 5

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 6

Which two steps belong in the Cortex XSOAR incident lifecycle? (Choose two.)

- A. Planning
- B. Incident creation
- C. Incident notification
- D. Preparation

Answer: AB

NEW QUESTION 7

Which response action in Cortex XSIAM would be unavailable to a SOC analyst investigating an incident involving a Linux server?

- A. File search and destroy
- B. Live Terminal session initiation
- C. Running a script
- D. Halting network access

Answer: A

NEW QUESTION 8

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 Stitching is 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 the Causality 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 Analytics uses the 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 9

Where can an administrator begin to grant a new non-SSO user access to a Cortex XDR tenant? (Choose one answer)

- A. Customer Support Portal
- B. Cortex Gateway
- C. Cortex XDR tenant settings under Access Management
- D. IT Service Portal

Answer: B

Explanation:

The Cortex Gateway (formerly known as the Cortex Hub) serves as the centralized management plane for all Palo Alto Networks Cortex applications, including XDR, XSIAM, and XSOAR.

User Management: For non-SSO users, the process of granting access starts at the Gateway level. An administrator logs into the Gateway to create the user account and then selects the specific tenant the user should have access to.

Role Assignment: Once the user is added to the Gateway, the administrator can then assign the specific administrative or analyst roles required for that user within the tenant.

Why others are incorrect: While the Customer Support Portal (A) is used for licensing and support cases, and Access Management (C) is where you define the permissions within the tenant, the actual "beginning" of granting access for a new account typically happens at the Gateway level to ensure the user identity exists in the Palo Alto cloud ecosystem first.

NEW QUESTION 10

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 10

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 14

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 15

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 20

How can an administrator run a Cortex XSOAR playbook regularly at a specific time and day of the week?

- A. By configuring the playbook to run on a specific date and time
- B. By creating a job that will run the playbook
- C. By creating a scheduled report that will run the playbook
- D. By creating a script that will run the playbook

Answer: B

NEW QUESTION 22

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 26

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 30

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SecOps-Pro Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SecOps-Pro Product From:

<https://www.2passeasy.com/dumps/SecOps-Pro/>

Money Back Guarantee

SecOps-Pro Practice Exam Features:

- * SecOps-Pro Questions and Answers Updated Frequently
- * SecOps-Pro Practice Questions Verified by Expert Senior Certified Staff
- * SecOps-Pro Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SecOps-Pro Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year