

# Paloalto-Networks

## Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional



#### NEW QUESTION 1

Which Cortex XDR Exploit Prevention Module (EPM) is specifically designed to detect and block "Return-Oriented Programming" (ROP) techniques by monitoring for "stack pivoting" or "jump to return" instructions?

- A. Anti-Exploit Core
- B. JMP2RET / Stack Pivot Protection
- C. Local Privilege Escalation Protection
- D. DLL Security

**Answer:** B

#### 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

How do sensors function in Cortex XSIAM?

- A. They monitor endpoint agent health.
- B. They monitor data ingestion health.
- C. They assist with log stitching.
- D. They collect logs and telemetry data.

**Answer:** D

#### NEW QUESTION 5

In which scenario would an organization benefit from Cortex XDR compared to an EDR solution?

- A. A business wants to integrate data from network traffic, cloud environments, and identity systems for a unified threat landscape.
- B. A corporation wants to monitor endpoint activities for advanced threats and gain visibility into endpoint behaviors.
- C. A customer relies on manual processes for incident detection and response with minimal use of automated tools and analytics.
- D. A company requires endpoint security that focuses on isolating and responding to threats at the endpoint level.

**Answer:** A

#### NEW QUESTION 6

Why would a security engineer be unable to activate Cortex XDR analytics when configuring data sources and alert sensors during a Cortex XSIAM evaluation? (Choose one answer)

- A. The engineer needs to install the Analytics engine.
- B. Pathfinder must be activated before turning on analytics.
- C. Baseline requirements must be met before activating analytics.
- D. The engineer still needs to activate the identity Analytics engine.

**Answer:** C

#### NEW QUESTION 7

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 8

Which Cortex XDR component raises an alert when suspicious activity composed of multiple events is detected and deviates from established baseline behavior?

- A. Analytics Engine
- B. Causality Analysis Engine
- C. XQL Query Engine
- D. Cloud Identity Engine

**Answer:** A

#### NEW QUESTION 9

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 10

Which Cortex XSIAM feature uses machine learning to automatically group related alerts into a single, manageable incident to reduce alert fatigue?

- A. XDM Mapping
- B. Alert Stitching
- C. Incident Stitching
- D. Analytics Engine

**Answer:** C

#### Explanation:

Incident Stitching(or Correlation) is the intelligence layer in Cortex XSIAM that addresses the "swamping" of SOC analysts with too many individual alerts.

Clustering:It analyzes incoming alerts from disparate sources and uses machine learning to identify if they belong to the same attack story based on shared entities (e.g., same host, same user, same IP) and timeframes.

Contextualization:Instead of seeing 50 separate "Suspicious Process" and "Malicious URL" alerts, the analyst sees oneIncidentthat contains all 50 alerts. This provides a clear picture of the attack's progression and drastically reduces the number of "tickets" an analyst needs to review.

#### NEW QUESTION 10

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 13

An analyst wants to create a detection rule that triggers when any process attempts to perform code injection into thelsass.exe process, regardless of whether the file hash of the source process is known to be malicious. Which type of rule should be created?

- A. IOC (Indicator of Compromise)
- B. BIOC (Behavioral Indicator of Compromise)
- C. Correlation Rule
- D. Analytics Alert

**Answer:** B

#### NEW QUESTION 18

Which Cortex XSOAR feature is used to ensure that specific data points from an incoming alert (such as a "Source\_Address" from a firewall log) are correctly assigned to the standardized "Source IP" field within the XSOAR incident?

- A. Classification
- B. Mapping
- C. Data Normalization
- D. Playbook Transformation

**Answer:** B

#### Explanation:

In Cortex XSOAR, the process of handling incoming data involves two distinct steps:ClassificationandMapping.

Classification:Determineswhatthe incident is (e.g., "This is a Phishing incident").

Mapping (B):Once the incident type is known, Mapping is used to "link" the raw data from the source integration to the fields in the XSOAR incident. For example, if a third-party tool sends an IP in a field called src, theMapperensures that value is placed into the XSOAR incident field sourceip.

Consistency:This ensures that regardless of which tool detected the threat, the analyst and the playbooks always see the data in the same standardized fields, which is essential for automation to work correctly.

#### NEW QUESTION 19

Which two statements are relevant to reports in Cortex XDR? (Choose two.)

- A. They can be sent in a password protected PDF version.
- B. They can be automatically pushed to the corporate intranet.
- C. They can use mock data for visualization.
- D. They can have an attached screenshot of an XQL query widget.

**Answer:** AD

#### NEW QUESTION 22

What is the primary objective of a "Tier 1" analyst during the triage process?

- A. Performing deep-dive memory forensics on a compromised server.
- B. Negotiating with ransomware actors to recover encrypted data.
- C. Determining the validity of an alert and its urgency for escalation.
- D. Rewriting the company's information security policy.

**Answer:** C

#### NEW QUESTION 25

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 as insider threats, credential theft, and lateral movement.

Behavioral Baseline: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 the actions of the user account to find malicious intent.

#### NEW QUESTION 30

What is the role of content packs in Cortex XSOAR?

- A. To provide pre-built bundles for supporting security orchestration use cases
- B. To support technical support teams with relevant information required to troubleshoot
- C. To serve as a central location for installing, exchanging, and contributing content
- D. To serve as a major software versioning update

**Answer:** A

#### Explanation:

In Cortex XSOAR, Content Packs are the essential building blocks used to implement security orchestration, automation, and response (SOAR) workflows.

Pre-built Bundles:A content pack is a comprehensive, version-controlled bundle that includes all the components necessary for a specific security use case. This typically includes integrations (to connect to 3rd party tools), playbooks (the logic of the workflow), automation scripts, layouts, fields, and dashboards.

Rapid Deployment:Instead of building a phishing response workflow from scratch, an administrator can install the "Phishing" content pack from the Marketplace. This immediately provides the out-of-the-box (OOTB) logic required to handle that specific threat.

Note on Option C:While Option C describes the Cortex XSOAR Marketplace itself, the role of the content pack is the actual delivery of the pre-built logic and tools defined in Option A.

#### NEW QUESTION 31

Which scripting language will allow the use of the Query Builder in Cortex XDR to show the top five accounts with failed Windows logons in the past 24 hours? (Choose one answer)

- A. PowerShell
- B. JavaScript
- C. XQL
- D. Python

**Answer:** C

#### NEW QUESTION 35

A new incident in Cortex XSIAM contains WildFire malware and Behavioral Threat Protection (BTP) alerts about an unsigned process attempting to dump the memory of lsass.exe. Which initial verdict applies to this incident?

- A. False positive
- B. True positive
- C. False negative
- D. True negative

**Answer:** B

**NEW QUESTION 38**

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 42**

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 46**

Which task should a threat hunter include in the investigation when a Cortex XDR incident contains alerts about a malicious process?

- A. Immediately isolate the endpoint and delete the identified file.
- B. Search for the SHA256 file hash on other endpoints in the environment.
- C. Add the SHA256 file hash to the Cortex XDR global block list.
- D. Disable the account of the user responsible for initiating the process.

**Answer:** B

**NEW QUESTION 50**

Which scripting language would create a custom widget in Cortex XDR that shows the top five accounts with failed Windows logons in the past 24 hours?

- A. XQL
- B. JavaScript
- C. Python
- D. PowerShell

**Answer:** A

**NEW QUESTION 53**

Which activities are facilitated through the War Room in Cortex XSOAR? (Choose one answer)

- A. Running security playbooks, scripts, and commands
- B. Creating, editing, and deleting tasks in the workplan
- C. Viewing a summary of case details and alerts
- D. Conducting initial investigation of incident data and threat intelligence

**Answer:** A

**Explanation:**

The War Room in Cortex XSOAR is the primary collaborative workspace where analysts interact with an incident in real-time. It acts as a digital "command center" for the investigation.

**CLI and Command Execution:** The most defining feature of the War Room is the command-line interface (CLI) at the bottom. This allows analysts to run scripts and integration commands (e.g., !ad-disable-user or !vt-get-url) directly.

**Collaboration:** It provides a central log of every action taken. When multiple analysts work on a single incident, they can see each other's commands, notes, and the outputs of automated tasks, similar to a chat application but enriched with security data.

**Evidence Collection:** Every command run and every result returned in the War Room can be marked as evidence, which is then automatically compiled into the final incident report.

**Why other options are incorrect:**

Option B: Managing the "to-do" list of an incident (creating/editing tasks) is done in the Workplan tab.

Option C: High-level overviews and summaries are found in the Incident Info or Dashboard views.

Option D: While investigation happens here, "initial investigation" is usually a function of the Classification and Mapping phase or the Incident Summary view before an analyst dives into the manual command execution of the War Room.

**NEW QUESTION 57**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SecOps-Pro Practice Test Here](#)**