

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

Which two types of tasks are supported in Cortex XSIAM playbooks? (Choose two answers)

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

Answer: BD

NEW QUESTION 3

What is the primary benefit of "Platformization"—the consolidation of disparate security tools into a unified platform like Cortex—for a modern SOC?

- A. Increasing the total number of alerts to ensure maximum visibility.
- B. Reducing the complexity of the security stack and improving data correlation.
- C. Completely eliminating the need for human analysts in the SOC.
- D. Allowing every business department to manage its own security tools independently.

Answer: B

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

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 6

What is the function of a Causality View?

- A. To provide users access to collaborate and execute CLI commands in Cortex XDR and Cortex XSIAM
- B. To present the alerts and process execution chain of all activity pertaining to the same event
- C. To consolidate multiple security tools into a single interface to improve analyst productivity
- D. To present alerts from multiple data sources as individual incidents in the console

Answer: B

NEW QUESTION 7

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 8

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 9

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

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 10

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 15

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 16

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 19

Where is the data retrieved by an integration task (such as a user's email address or a file's reputation) stored within an incident so that other playbook tasks can access it?

- A. War Room
- B. Context Data
- C. Incident Fields
- D. Evidence Board

Answer: B

NEW QUESTION 20

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 25

During which phase of the NIST Incident Response lifecycle does a SOC team conduct a "Lessons Learned" meeting to improve future response efforts?

- A. Preparation
- B. Detection and Analysis
- C. Containment, Eradication, and Recovery
- D. Post-Incident Activity

Answer: D

NEW QUESTION 26

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 27

What is enabled by Role-Based Access Control (RBAC) in Cortex XDR?

- A. Management of permissions and assignment of administrator access rights.
- B. Ability to manage Cortex XDR features based on job function.
- C. Automated response to detected threats based on user roles.
- D. Granular control and visibility over network traffic policies based on user roles.

Answer: A

NEW QUESTION 31

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 35

Which SOC role investigates a new low severity alert? (Choose one answer)

- A. SOC manager
- B. Threat hunter

- C. Triage specialist
- D. Incident responder

Answer: C

NEW QUESTION 39

A company has a highly segmented network where the Cortex XSOAR server cannot directly communicate with an on-premises mail server. Which component should be deployed in the mail server's segment to facilitate integration?

- A. Broker VM
- B. XSOAR Engine
- C. Cortex Gateway
- D. XSOAR Proxy

Answer: B

NEW QUESTION 44

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 46

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)