

Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional



NEW QUESTION 1

Which action should an administrator take to create automated response actions when a user account is compromised? (Choose one answer)

- A. Map the events as a type of Cortex XSOAR incident, then run a playbook.
- B. Run a custom script from the Cortex XDR script library.
- C. Create a script in Cortex XSOAR that will run a playbook based on the scenario.
- D. Create playbook triggers in Cortex XSIAM and run playbooks for each alert.

Answer: A

NEW QUESTION 2

Which Cortex XSIAM component uses machine learning to automatically build a baseline of "normal" behavior for every user and host in the network, and then provides a searchable profile of their historical activity and risk level?

- A. XQL Engine
- B. Entity Profiling
- C. Broker VM
- D. Data Ingestion Service

Answer: B

Explanation:

Entity Profiling is the specific Cortex XSIAM capability that powers its User and Entity Behavioral Analytics (UEBA) functions.

Baselining: For every entity (a user account or a host/device), the system observes its standard operations—such as which servers it connects to, what time it typically logs in, and what applications it runs.

Searchable Profiles: Analysts can use the Entity Explorer to view a "Profile" for any user. This profile includes a "Risk Score" and a summary of all anomalies associated with that entity over time.

Security Context: This allows a SOC analyst to quickly answer the question: "Is this user's current behavior (e.g., accessing a sensitive database) normal for them, or is it a sign of credential theft?"

Difference from XQL (A): XQL is the language used to query the data, but Entity Profiling is the background process and engine that builds the behavioral models and stores the entity-specific context.

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 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

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 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 one incident that 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 12

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 16

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 19

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 21

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 22

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 25

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:

The War Room is 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, the conversation and collaboration happen exclusively within the War Room interface.

Correction: Corrected "analystsle" to "analysts are able."

NEW QUESTION 29

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 33

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 38

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 40

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 43

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 45

What is required to enable ingestion of on-premises firewall logs into Cortex XDR?

- A. Broker VM
- B. API
- C. PAN-OS content pack
- D. Cloud Identity Engine

Answer: A

Explanation:

To get logs from on-premises hardware into the cloud-native Cortex Data Lake, a "bridge" is required. This is the role of the Broker VM.

Local Collector: The Broker VM is a virtual machine (running on ESXi or Hyper-V) that sits inside your local network. It acts as a local syslog server, NetFlow collector, or Windows Event collector.

Secure Forwarding: It receives the raw logs from on-premises firewalls, compresses and encrypts them, and then securely uploads them to the Cortex Data Lake.

Management: It also serves as a proxy for the Cortex XDR agents and helps with tasks like Local Scanning and Directory Sync. Without the Broker VM, on-premises firewalls that cannot natively reach the cloud would have no way to contribute their data to the XDR "stitching" process.

NEW QUESTION 47

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 50

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 51

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 54

.....

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](#)