

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 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 3

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 4

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 5

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 6

A file hash is evaluated in Cortex XSOAR by using two unique threat feeds: VirusTotal feed (rating of B- usually reliable) and the file verdict is malicious AlienVault feed (rating of B- usually reliable) and the file verdict is benign What is the file verdict in XSOAR?

- A. Benign
- B. Malicious
- C. Unknown
- D. Suspicious

Answer: B

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 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 9

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 10

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 10

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 11

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 12

How does the "Unit 42 Intel" integration directly assist a SOC analyst within the Cortex XDR or XSIAM Incident view?

- A. It automatically resets the user's password in Active Directory.
- B. It provides a "threat card" with actor profiles, known aliases, and related MITRE ATT&CK techniques.
- C. It opens a 24/7 chat window with a dedicated Unit 42 forensic investigator.
- D. It provides the source code of the malware identified in the incident.

Answer: B

NEW QUESTION 13

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 18

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 19

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

When writing a custom XQL query to hunt for specific network anomalies, which part of the query syntax is used to define the specific table or source of data being searched?

- A. filter
- B. dataset
- C. fields
- D. comp

Answer: B

Explanation:

In the XQL (Cortex Query Language) syntax, every query must begin with the dataset stage.

Data Source Identification: The dataset command tells the engine exactly where to look within the Cortex Data Lake. For example, dataset = xdr_data targets endpoint and network logs, while dataset = pan_os_logs targets firewall logs specifically.

Query Structure: Without a defined dataset, the query engine has no context for the fields or filters that follow. Once the dataset is established, you then use pipes (|) to add stages like filter (to narrow results), fields (to select columns), and comp (to perform calculations/aggregations).

NEW QUESTION 24

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: Classification and Mapping.

Classification: Determines what the 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, the Mapper ensures 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 25

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 27

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 31

During a sophisticated cyber attack, a company experiences a stealthy, multivector intrusion that evades detection by traditional security tools. The company requires a solution that will correlate and analyze the disparate attack indicators across its network, endpoints, and cloud environments to uncover the full scope of the breach and take immediate automated response actions. Which solution should be recommended?

- A. XDR
- B. SIEM
- C. EDR
- D. XSOAR

Answer: A

NEW QUESTION 35

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 38

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 40

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 44

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 49

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 50

.....

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](#)