Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

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
In the MITRE ATT&CK framework, which term describes the specific high-level "Why" or goal of an attacker, such as "Initial Access" or "Exfiltration"?

A. Technique
B. Tactic
C. Procedure
D. Mitigation

Answer: B

Explanation:
TheMITRE ATT&CKframework is categorized into a hierarchy that helps SOC analysts understand attacker behavior:
Tactic (B):This is theobjective/goalof the attacker. There are currently 14 tactics in the Enterprise matrix, including Reconnaissance, Persistence, and Lateral Movement. It answers the question "What is the attacker trying to achieve?"
Technique (A):This is the "How"—the specific method used to achieve a tactic (e.g., "Spearphishing Attachment" to achieve "Initial Access").
Procedure (C):The specific implementation or "recipe" used by a particular threat actor (e.g., "APT28 used a specific PowerShell script to bypass AMSI").
Mapping:Cortex XDR and XSIAM natively map alerts to these Tactics and Techniques to help analysts quickly understand the stage and intent of an attack.

NEW QUESTION 3
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 4
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 5
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 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 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 9
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 Stitchingis 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 theCausality 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 Analyticsusesthe 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 10
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 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 11
Which two types of content can be installed or upgraded through a Cortex XSIAM content pack? (Choose two.)

A. Analytics alerts
B. Playbook triggers
C. Data Model rules
D. Behavioral Threat Protection (BTP)

Answer: AC

NEW QUESTION 13
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 15
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 19
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 24
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 theXQL (Cortex Query Language)syntax, every query must begin with thedatasetstage.
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 27
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 32
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:
TheWar Roomis 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, theconversation and collaborationhappen exclusively within the War Room interface.
Correction:Corrected "analystsle" to "analysts are able."

NEW QUESTION 35

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 38
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 asinsider threats, credential theft, and lateral movement.
Behavioral Baselining: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 theactions of the user accountto find malicious intent.

NEW QUESTION 41
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 Packsare 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 theCortex XSOAR Marketplaceitself, therole of the content packis the actual delivery of the pre-built logic and tools defined in Option A.

NEW QUESTION 45
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 50
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 53
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 58
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 62
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 63
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 64
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 69
.....

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