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
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
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 14
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 18

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 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 23
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 25
What is a difference between cold storage and hot storage in Cortex?

A. Cold storage is required, while hot storage is optional.
B. Cold storage and hot storage can be stored in different cloud locations.
C. Logs in cold storage have more details than logs stored in hot storage.
D. Querying logs in cold storage takes more time than querying logs in hot storage.

Answer: D

NEW QUESTION 29
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 32
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 theBroker 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 34
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 36
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 37
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 39
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:
TheWar Roomin 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 runscriptsandintegration 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 theWorkplantab.
Option C:High-level overviews and summaries are found in theIncident InfoorDashboardsviews.
Option D:While investigation happens here, "initial investigation" is usually a function of theClassification and Mappingphase or theIncident Summaryview before an analyst dives into the manual command execution of the War Room.

NEW QUESTION 42
.....

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