Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

https://www.2passeasy.com/dumps/SecOps-Pro/

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 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
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 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
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 7
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 8
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 9
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 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 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 10
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 12
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 17
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 20
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 22
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 26
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 31
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 35
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SecOps-Pro Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SecOps-Pro Product From:

https://www.2passeasy.com/dumps/SecOps-Pro/

Money Back Guarantee

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