Paloalto Networks

SecOps-Pro

Palo Alto Networks Security Operations Professional

Latest Version: 6.1

Question: 1

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.

Question: 2

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

Explanation:
In Cortex XDR, Role-Based Access Control (RBAC) is the primary mechanism for enforcing the principle of least privilege within the management console. It allows organizations to define exactly what an administrator or analyst can see and do.
Permissions Management: RBAC allows the "Account Admin" to create or use predefined roles (such as Security Admin, Instance Admin, or Viewer) that grant specific permissions for various actions like viewing alerts, performing remediation (isolating endpoints), or configuring malware profiles.
Assignment of Rights: These roles are then assigned to users or groups (often synced via SAML/Active Directory). This ensures that a Tier 1 analyst might have "View Only" rights for certain logs, while a Tier 3 analyst or SOC Manager has the rights to execute scripts or initiate Live Terminal sessions.
Distinction from Network Policies: Unlike firewall rules (Option D), RBAC in Cortex XDR specifically governs administrative access to the platform itself, not the flow of user traffic across the network.

Question: 3

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

Explanation:
In Cortex XSOAR, Jobs are the dedicated mechanism used to automate tasks that are not triggered by an incoming security event/incident.
Scheduling Mechanism: Jobs allow an administrator to schedule the execution of a specific playbook or script at recurring intervals. This is configured using a calendar-based UI or standard Cron expressions (e.g., "Run every Monday at 08:00").
Use Cases: Common use cases for Jobs include daily health checks of integrations, weekly cleanup of indicators, or pulling recurring reports from third-party intelligence sources.

Playbook Execution: When a Job runs, it creates an incident (or works within a recurring framework) to execute the assigned playbook, ensuring that the SOC workflow is maintained even without an external trigger.
Why other options are incorrect:
Option A: Playbooks themselves do not have internal "timers" to start; they require a trigger (an incident, a manual start, or a Job).
Option C: Reports are used for data visualization and export; while they can be scheduled, they are not the mechanism used to trigger operational playbooks.
Option D: While a script can perform actions, it still needs a Job to trigger it on a recurring schedule.

Question: 4

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.

Question: 5

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

Explanation:
Threat hunting is a proactive and investigative process that differs from immediate incident response/remediation. When a malicious process is identified, a threat hunter's primary goal is to determine the scope and impact of the threat across the entire enterprise.
Scoping the Attack: By searching for the specific SHA256 file hash on other endpoints, the hunter can identify if the threat has spread (lateral movement) or if it exists elsewhere in a dormant state (persistence). This helps determine if the incident is an isolated event or part of a wider campaign.
Evidence Gathering: This task allows the analyst to see if the file behaves differently on different hosts or if it was introduced via a common vector (like a shared network drive or a widespread email).
Why others are incorrect: Options A, C, and D are remediation actions. While they may eventually be necessary, the specific "hunting" task is the act of searching for the indicator (the hash) across the environment to understand the full extent of the breach.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer