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 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 Profilingis 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 theEntity Explorerto 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 forthem, or is it a sign of credential theft?"
Difference from XQL (A):XQL is the language used toquerythe data, but Entity Profiling is the background process and engine thatbuildsthe behavioral models and stores the entity-specific context.

NEW QUESTION 3
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 4
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 5
What is a primary responsibility of an incident responder in a SOC?

A. Mitigating incidents that have been escalated
B. Supervising vulnerability assessments and penetration tests
C. Determining or adjusting criticality of alerts
D. Developing incident recovery crises communications plans

Answer: A

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
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 9
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 10
Which dashboard or module in Cortex XSIAM provides visibility into unmanaged devices, unauthorized shadow IT, and cloud assets that do not currently have a Cortex agent installed?

A. Host Insights
B. Asset Inventory
C. Cloud Discovery & Exposure
D. Identity Analytics

Answer: C

NEW QUESTION 10
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 14
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 19
Where can an administrator begin to grant a new non-SSO user access to a Cortex XDR tenant? (Choose one answer)

A. Customer Support Portal
B. Cortex Gateway
C. Cortex XDR tenant settings under Access Management
D. IT Service Portal

Answer: B

Explanation:
TheCortex Gateway(formerly known as the Cortex Hub) serves as the centralized management plane for all Palo Alto Networks Cortex applications, including XDR, XSIAM, and XSOAR.
User Management:For non-SSO users, the process of granting access starts at the Gateway level. An administrator logs into the Gateway to create the user account and then selects the specific tenant the user should have access to.
Role Assignment:Once the user is added to the Gateway, the administrator can then assign the specific administrative or analyst roles required for that user within the tenant.
Why others are incorrect:While the Customer Support Portal (A) is used for licensing and support cases, and Access Management (C) is where you define thepermissionswithin the tenant, the actual "beginning" of granting access for a new account typically happens at the Gateway level to ensure the user identity exists in the Palo Alto cloud ecosystem first.

NEW QUESTION 24
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 27
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 28
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 32
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:ClassificationandMapping.
Classification:Determineswhatthe 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, theMapperensures 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 33
What is the WildFire verdict on a sample that does not pose a direct security threat, but is shown to display obtrusive behavior?

A. Grayware
B. Unknown
C. Benign
D. Malware

Answer: A

NEW QUESTION 37
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 39
Which solution will minimize mean time to resolution (MTTR) when, as a result of previous malware infection, a company??s Windows endpoint is suffering a small amount of file corruption and modified registry keys?

A. Issue a new laptop from the help desk to expedite a clean system.
B. Use Live Terminal to connect to the machine and upload files to replace the corrupted files.
C. Use group policy objects to push new files and registry key changes to the endpoint.
D. Use remediation suggestions to restore the affected files and registry modifications.

Answer: D

NEW QUESTION 40
.....

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