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
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 3
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 4
How do sensors function in Cortex XSIAM?

A. They monitor endpoint agent health.
B. They monitor data ingestion health.
C. They assist with log stitching.
D. They collect logs and telemetry data.

Answer: D

NEW QUESTION 5
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 6
An analyst identifies that a custom internal application is being incorrectly flagged as malicious by the Behavioral Threat Protection (BTP) module. What is the best way to stop these alerts while maintaining security for other applications?

A. Disable the BTP module in the endpoint's Malware Profile.
B. Add the application's file hash to the Global Block List.
C. Create a specific Exception for the alert from the Incident View.
D. Move the endpoint to a policy group with no security profiles.

Answer: C

Explanation:
In Cortex XDR,Exceptionsare the preferred method for tuning the platform to reduce false positives without creating broad security gaps.
Granular Control:When you create an exception from a specific alert, Cortex XDR allows you to define the scope based on specific attributes like the process name, command line, or file path.
Targeted Tuning:Unlike disabling an entire module (Option A), an exception only ignores the specific behavior for that specific application.
Ease of Use:This can be done directly from the "Check Action" or "Alerts" tab within an incident, allowing the analyst to quickly suppress future occurrences of that specific false positive.

NEW QUESTION 7
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 8
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 9
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 10
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 10
Which process in Cortex XSIAM ensures that raw logs from different vendors (e.g., Check Point, Cisco, and Microsoft) are converted into a standardized format for unified analysis?

A. Data Stitching
B. XDM Mapping
C. Entity Profiling
D. Log Ingestion

Answer: B

Explanation:
TheXDM (Cortex Data Model)is the backbone of Cortex XSIAM's ability to act as a unified SOC platform.
Standardization:Raw logs come in many formats (Syslog, JSON, LEEF).XDM Mappingis the process of taking those raw fields and "mapping" them to a common schema. For example, "src_ip," "source_address," and "sIP" from different vendors are all mapped to a single XDM field called xdm.source.ipv4.
Cross-Vendor Correlation:Once data is mapped to XDM, an analyst can write one XQL query that searches across logs fromallvendors simultaneously, which is essential for effective threat hunting in a multi-vendor environment.

NEW QUESTION 15
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 20
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 21
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 26
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 27
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 31
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 36
During a sophisticated cyber attack, a company experiences a stealthy, multivector intrusion that evades detection by traditional security tools. The company requires a solution that will correlate and analyze the disparate attack indicators across its network, endpoints, and cloud environments to uncover the full scope of the breach and take immediate automated response actions. Which solution should be recommended?

A. XDR
B. SIEM
C. EDR
D. XSOAR

Answer: A

NEW QUESTION 37
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 39
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 41
.....

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