Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

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 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 3
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 4
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 5
According to the Traffic Light Protocol (TLP) 2.0 standard, which classification is used for information that is restricted to the specific individuals involved in an investigation and cannot be shared further?

A. TLP:CLEAR
B. TLP:GREEN
C. TLP:AMBER
D. TLP:RED

Answer: D

NEW QUESTION 6
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 7
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 8
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 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 11
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 15
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 18
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 19
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 23
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 28
Which two statements are relevant to reports in Cortex XDR? (Choose two.)

A. They can be sent in a password protected PDF version.
B. They can be automatically pushed to the corporate intranet.
C. They can use mock data for visualization.
D. They can have an attached screenshot of an XQL query widget.

Answer: AD

NEW QUESTION 31
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 34
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 39
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 42
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 47
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 49
Which response action in Cortex XDR allows a SOC analyst to remotely access an endpoint??s command-line interface to perform manual forensic data collection or system remediation?

A. Remote Shell
B. Live Terminal
C. Action Center
D. Python Console

Answer: B

Explanation:
Live Terminalis a powerful forensic and remediation tool built directly into the Cortex XDR and XSIAM consoles.
Direct Access:It provides a secure, web-based terminal session to a remote endpoint (Windows, macOS, or Linux) without requiring RDP or SSH to be enabled on the target.
Capabilities:Analysts can browse the file system, terminate processes, download/upload files, and execute PowerShell or Bash commands.
Auditability:Every action taken during a Live Terminal session is logged and recorded, ensuring that there is a full audit trail for compliance and "chain of custody" purposes during an investigation.
Why others are incorrect:TheAction Center (C)is where you monitor the status of pending or completed actions (like a scan or isolation request), but it is not the interface used to execute the commands themselves.

NEW QUESTION 50
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 54
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 58
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 63
.....

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