Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

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

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
In the MITRE ATT&CK framework, which term describes the specific high-level "Why" or goal of an attacker, such as "Initial Access" or "Exfiltration"?

A. Technique
B. Tactic
C. Procedure
D. Mitigation

Answer: B

Explanation:
TheMITRE ATT&CKframework is categorized into a hierarchy that helps SOC analysts understand attacker behavior:
Tactic (B):This is theobjective/goalof the attacker. There are currently 14 tactics in the Enterprise matrix, including Reconnaissance, Persistence, and Lateral Movement. It answers the question "What is the attacker trying to achieve?"
Technique (A):This is the "How"—the specific method used to achieve a tactic (e.g., "Spearphishing Attachment" to achieve "Initial Access").
Procedure (C):The specific implementation or "recipe" used by a particular threat actor (e.g., "APT28 used a specific PowerShell script to bypass AMSI").
Mapping:Cortex XDR and XSIAM natively map alerts to these Tactics and Techniques to help analysts quickly understand the stage and intent of an attack.

NEW QUESTION 3
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 4
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 5
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 6
Which response action in Cortex XSIAM would be unavailable to a SOC analyst investigating an incident involving a Linux server?

A. File search and destroy
B. Live Terminal session initiation

C. Running a script
D. Halting network access

Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 14
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 17

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 21
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 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 27
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 32
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 36
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 39
.....

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