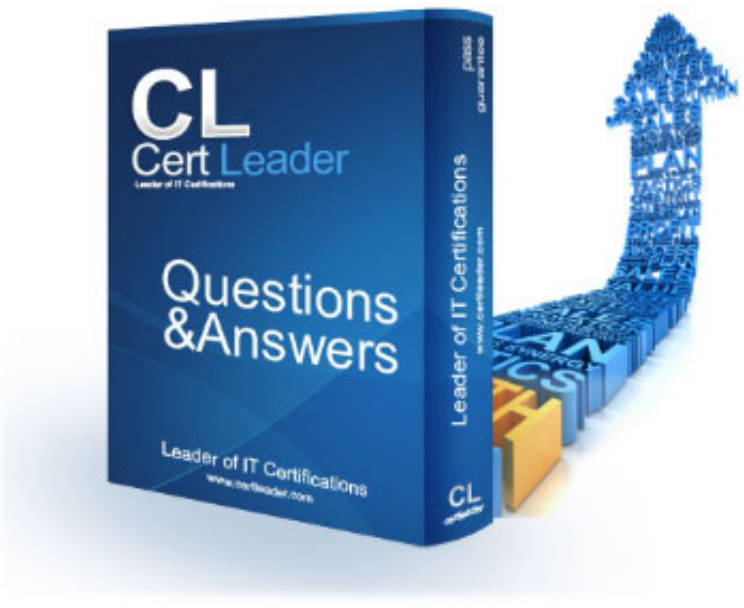
SecOps-Pro Dumps

Palo Alto Networks Security Operations Professional

https://www.certleader.com/SecOps-Pro-dumps.html



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
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 steps belong in the Cortex XSOAR incident lifecycle? (Choose two.)

A. Planning
B. Incident creation
C. Incident notification
D. Preparation

Answer: AB

NEW QUESTION 5
Which Cortex XDR component raises an alert when suspicious activity composed of multiple events is detected and deviates from established baseline behavior?

A. Analytics Engine
B. Causality Analysis Engine
C. XQL Query Engine
D. Cloud Identity Engine

Answer: A

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
Where in Cortex XSOAR are analysts able to collaborate and converse with others for joint real-time investigations?

A. Investigations tab
B. War Room
C. Evidence Board
D. Work plan

Answer: B

Explanation:
TheWar Roomis the central collaborative feature of Cortex XSOAR. It is designed to mimic a physical "war room" where security experts gather to solve a crisis.
Real-Time Collaboration:It features a chat-like interface where analysts can post notes, upload files, and tag other team members to collaborate on a specific incident in real-time.
Shared CLI:Every analyst in the War Room sees the commands being run by others and the results of those commands. This prevents duplication of effort and ensures everyone has the same context.
Note on Evidence Board (C):While the Evidence Board displays captured artifacts, theconversation and collaborationhappen exclusively within the War Room interface.
Correction:Corrected "analystsle" to "analysts are able."

NEW QUESTION 8
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 Packsare 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 theCortex XSOAR Marketplaceitself, therole of the content packis the actual delivery of the pre-built logic and tools defined in Option A.

NEW QUESTION 9
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 10
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 10
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 14
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 18
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 20
Which activities are facilitated through the War Room in Cortex XSOAR? (Choose one answer)

A. Running security playbooks, scripts, and commands
B. Creating, editing, and deleting tasks in the workplan
C. Viewing a summary of case details and alerts
D. Conducting initial investigation of incident data and threat intelligence

Answer: A

Explanation:
TheWar Roomin Cortex XSOAR is the primary collaborative workspace where analysts interact with an incident in real-time. It acts as a digital "command center" for the investigation.
CLI and Command Execution:The most defining feature of the War Room is the command-line interface (CLI) at the bottom. This allows analysts to runscriptsandintegration commands(e.g., !ad-disable-user or !vt-get-url) directly.
Collaboration:It provides a central log of every action taken. When multiple analysts work on a single incident, they can see each other's commands, notes, and the outputs of automated tasks, similar to a chat application but enriched with security data.
Evidence Collection:Every command run and every result returned in the War Room can be marked as evidence, which is then automatically compiled into the final incident report.
Why other options are incorrect:
Option B:Managing the "to-do" list of an incident (creating/editing tasks) is done in theWorkplantab.
Option C:High-level overviews and summaries are found in theIncident InfoorDashboardsviews.
Option D:While investigation happens here, "initial investigation" is usually a function of theClassification and Mappingphase or theIncident Summaryview before an analyst dives into the manual command execution of the War Room.

NEW QUESTION 21
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SecOps-Pro Exam with Our Prep Materials Via below:

https://www.certleader.com/SecOps-Pro-dumps.html