Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

NEW QUESTION 1
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 2
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 3
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 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
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 6
An analyst wants to create a detection rule that triggers when any process attempts to perform code injection into thelsass.exeprocess, regardless of whether the file hash of the source process is known to be malicious. Which type of rule should be created?

A. IOC (Indicator of Compromise)

B. BIOC (Behavioral Indicator of Compromise)
C. Correlation Rule
D. Analytics Alert

Answer: B

NEW QUESTION 7
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 8
Which component of Cortex XDR is designed to detect insider threats?

A. Forensics
B. Identity Analytics
C. Cloud Identity Engine
D. Host Insights

Answer: B

Explanation:
Identity Analytics(formerly part of the Magnifier module) is specifically designed to identify stealthy attacks that traditional signature-based tools miss, such asinsider threats, credential theft, and lateral movement.
Behavioral Baselining:It uses Machine Learning to create a "baseline" of normal behavior for every user and entity in the network. It tracks who they usually communicate with, what time they log in, and what resources they typically access.
Anomaly Detection:If a user suddenly begins accessing sensitive servers they??ve never touched before or starts transferring large amounts of data to an unusual external IP, Identity Analytics flags this as a "User Behavioral Analytics" (UBA) alert.
Focus on Identity:Unlike Host Insights (which looks at vulnerabilities) or Forensics (which looks at disk artifacts), Identity Analytics focuses purely on theactions of the user accountto find malicious intent.

NEW QUESTION 9
What is a difference between cold storage and hot storage in Cortex?

A. Cold storage is required, while hot storage is optional.
B. Cold storage and hot storage can be stored in different cloud locations.
C. Logs in cold storage have more details than logs stored in hot storage.
D. Querying logs in cold storage takes more time than querying logs in hot storage.

Answer: D

NEW QUESTION 10
During which phase of the NIST Incident Response lifecycle does a SOC team conduct a "Lessons Learned" meeting to improve future response efforts?

A. Preparation
B. Detection and Analysis
C. Containment, Eradication, and Recovery
D. Post-Incident Activity

Answer: D

NEW QUESTION 10
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 12
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 16
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 19
.....

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