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
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 5
Which Cortex XSIAM component uses machine learning to automatically build a baseline of "normal" behavior for every user and host in the network, and then provides a searchable profile of their historical activity and risk level?

A. XQL Engine
B. Entity Profiling
C. Broker VM
D. Data Ingestion Service

Answer: B

Explanation:
Entity Profilingis the specific Cortex XSIAM capability that powers its User and Entity Behavioral Analytics (UEBA) functions.
Baselining:For every entity (a user account or a host/device), the system observes its standard operations—such as which servers it connects to, what time it typically logs in, and what applications it runs.
Searchable Profiles:Analysts can use theEntity Explorerto view a "Profile" for any user. This profile includes a "Risk Score" and a summary of all anomalies associated with that entity over time.
Security Context:This allows a SOC analyst to quickly answer the question: "Is this user's current behavior (e.g., accessing a sensitive database) normal forthem, or is it a sign of credential theft?"
Difference from XQL (A):XQL is the language used toquerythe data, but Entity Profiling is the background process and engine thatbuildsthe behavioral models and stores the entity-specific context.

NEW QUESTION 6
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 7
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 8
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 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 12
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 17
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 20
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 25
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 30
What is the function of a Causality View?

A. To provide users access to collaborate and execute CLI commands in Cortex XDR and Cortex XSIAM
B. To present the alerts and process execution chain of all activity pertaining to the same event
C. To consolidate multiple security tools into a single interface to improve analyst productivity
D. To present alerts from multiple data sources as individual incidents in the console

Answer: B

NEW QUESTION 34
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 35
Which two functions are allowed when stitching logs in Cortex XDR? (Choose two.)

A. Providing real-time threat prevention or remediation of threats
B. Creating granular BIOC and correlation rules
C. Enabling creation of custom scripts for remediation of security incidents
D. Running investigation queries based on combined network and endpoint events

Answer: BD

NEW QUESTION 40
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 43
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 48
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 52
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 55
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 59
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 62
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 66
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 71
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 75
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 78
Which scripting language would create a custom widget in Cortex XDR that shows the top five accounts with failed Windows logons in the past 24 hours?

A. XQL
B. JavaScript
C. Python
D. PowerShell

Answer: A

NEW QUESTION 81
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 86
.....

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