Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

NEW QUESTION 1
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 2
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 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
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 12
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 16
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 17
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 18
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 21
Which metric is used by SOC management to measure the average "Dwell Time"—the duration between a successful compromise and the moment it is first identified by a security tool or analyst?

A. MTTR (Mean Time to Respond)
B. MTTA (Mean Time to Acknowledge)
C. MTTD (Mean Time to Detect)
D. MTTC (Mean Time to Contain)

Answer: C

NEW QUESTION 25
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 26
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 31
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 35
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 38
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 39
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 43
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 47
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 48
.....

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