Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

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

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 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 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
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
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 6
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 7
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 8
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 9
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 10
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 10
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 13
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 15
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 17
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 20
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 22
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 23
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 26
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 29
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 34
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 39
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 40
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 42
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 44
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 45
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 46
Which response action in Cortex XDR allows a SOC analyst to remotely access an endpoint??s command-line interface to perform manual forensic data collection or system remediation?

A. Remote Shell
B. Live Terminal
C. Action Center
D. Python Console

Answer: B

Explanation:
Live Terminalis a powerful forensic and remediation tool built directly into the Cortex XDR and XSIAM consoles.
Direct Access:It provides a secure, web-based terminal session to a remote endpoint (Windows, macOS, or Linux) without requiring RDP or SSH to be enabled on

the target.
Capabilities:Analysts can browse the file system, terminate processes, download/upload files, and execute PowerShell or Bash commands.
Auditability:Every action taken during a Live Terminal session is logged and recorded, ensuring that there is a full audit trail for compliance and "chain of custody" purposes during an investigation.
Why others are incorrect:TheAction Center (C)is where you monitor the status of pending or completed actions (like a scan or isolation request), but it is not the interface used to execute the commands themselves.

NEW QUESTION 51
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 54
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 57
.....

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