

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional

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



NEW QUESTION 1

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 2

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 3

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, Exceptions are 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 4

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:

The XDM (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 Mapping is 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 from all vendors simultaneously, which is essential for effective threat hunting in a multi-vendor environment.

NEW QUESTION 5

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 6

An analyst wants to create a detection rule that triggers when any process attempts to perform code injection into the `ssass.exe` process, 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 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 8

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 9

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 10

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 Packs are 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 the Cortex XSOAR Marketplace itself, the role of the content pack is the actual delivery of the pre-built logic and tools defined in Option A.

NEW QUESTION 10

Which scripting language will allow the use of the Query Builder in Cortex XDR to show the top five accounts with failed Windows logons in the past 24 hours? (Choose one answer)

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

Answer: C

NEW QUESTION 12

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 13

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 the Broker 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 15

.....

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