

Paloalto-Networks

Exam Questions SecOps-Pro

Palo Alto Networks Security Operations Professional



NEW QUESTION 1

What is a primary responsibility of an incident responder in a SOC?

- A. Mitigating incidents that have been escalated
- B. Supervising vulnerability assessments and penetration tests
- C. Determining or adjusting criticality of alerts
- D. Developing incident recovery crises communications plans

Answer: A

NEW QUESTION 2

In which scenario would an organization benefit from Cortex XDR compared to an EDR solution?

- A. A business wants to integrate data from network traffic, cloud environments, and identity systems for a unified threat landscape.
- B. A corporation wants to monitor endpoint activities for advanced threats and gain visibility into endpoint behaviors.
- C. A customer relies on manual processes for incident detection and response with minimal use of automated tools and analytics.
- D. A company requires endpoint security that focuses on isolating and responding to threats at the endpoint level.

Answer: A

NEW QUESTION 3

What is the primary benefit of "Platformization"—the consolidation of disparate security tools into a unified platform like Cortex—for a modern SOC?

- A. Increasing the total number of alerts to ensure maximum visibility.
- B. Reducing the complexity of the security stack and improving data correlation.
- C. Completely eliminating the need for human analysts in the SOC.
- D. Allowing every business department to manage its own security tools independently.

Answer: B

NEW QUESTION 4

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 5

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 6

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

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 8

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 9

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 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

During a sophisticated cyber attack, a company experiences a stealthy, multivector intrusion that evades detection by traditional security tools. The company requires a solution that will correlate and analyze the disparate attack indicators across its network, endpoints, and cloud environments to uncover the full scope of the breach and take immediate automated response actions. Which solution should be recommended?

- A. XDR
- B. SIEM
- C. EDR
- D. XSOAR

Answer: A

NEW QUESTION 14

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 19

A company has a highly segmented network where the Cortex XSOAR server cannot directly communicate with an on-premises mail server. Which component should be deployed in the mail server's segment to facilitate integration?

- A. Broker VM
- B. XSOAR Engine
- C. Cortex Gateway
- D. XSOAR Proxy

Answer: B

NEW QUESTION 20

.....

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

100% Actual & Verified — Instant Download, Please Click
[Order The SecOps-Pro Practice Test Here](#)