

# Palo Alto Networks SecOps-Generalist

**Palo Alto Networks Security Operations Generalist**

**For More Information – Visit link below:**

**<https://www.examsempire.com/>**

**Product Version**

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



**<https://examsempire.com/>**

**Visit us at: <https://www.examsempire.com/secops-generalist>**

# Latest Version: 6.0

## Question: 1

What is the purpose of log stitching in Cortex XDR?

Response:

- A. To correlate different log sources into a unified attack storyline
- B. To compress large log files for easier storage
- C. To remove duplicate log entries for better performance
- D. To automatically archive logs after 30 days

**Answer: A**

## Question: 2

An alert is triggered in Cortex XDR indicating that PowerShell is being used to execute commands remotely. The analyst investigates and confirms that the activity is expected administrator behavior. What type of alert classification is this?

Response:

- A. True Positive
- B. False Positive
- C. False Negative
- D. Benign Positive

**Answer: B**

## Question: 3

How does Cortex XSIAM enhance proactive security operations?

Response:

- A. By enabling AI-powered threat hunting and anomaly detection
- B. By automatically blocking all external network traffic
- C. By eliminating the need for EDR solutions
- D. By focusing only on known attack signatures

**Answer: A**

### Question: 4

The War Room in Cortex XSOAR is used for:

Response:

- A. Collaborative real-time investigation and response to security incidents
- B. Running playbooks automatically without human intervention
- C. Storing all historical threat intelligence reports
- D. Generating compliance reports for regulatory audits

**Answer: A**

### Question: 5

Your team is responsible for configuring Cortex XDR to improve compliance reporting. Your organization needs to meet GDPR data protection standards. Which of the following actions would be most effective?  
Response:

- A. Enable encryption for all stored logs
- B. Allow public access to compliance dashboards for transparency
- C. Disable all logging to avoid storing personal data
- D. Use default Cortex XDR configurations without changes

**Answer: A**

### Question: 6

Causality View in Cortex XDR provides analysts with:

Response:

- A. A visual representation of how a security event evolved over time
- B. Automatic remediation capabilities for all detected threats
- C. The ability to ignore false positives without investigation
- D. A simple list of alert logs without additional correlation

**Answer: A**

### Question: 7

Which of the following is a characteristic of a "true positive" security alert?

Response:

- A. An alert is triggered for a real threat that needs response
- B. An alert is incorrectly flagged as malicious but is actually benign
- C. A malicious attack occurs but is not detected
- D. An alert is ignored because it is too frequent

**Answer: A**

### Question: 8

Log stitching in Cortex XDR is used for:  
Response:

- A. Automatically blocking all detected threats
- B. Correlating multiple security events to create a unified incident timeline
- C. Encrypting security logs for compliance purposes
- D. Aggregating network traffic data only

**Answer: B**

### Question: 9

A SOC analyst receives an alert about a suspicious IP address attempting multiple login attempts across several endpoints. The analyst wants to automate the process of gathering intelligence on the IP before escalating the case.  
Which Cortex XSOAR feature should be used to automate this enrichment process?  
Response:

- A. A Playbook that queries threat intelligence feeds and correlates IOCs
- B. Manually searching the IP address on different threat intelligence platforms
- C. Running a forensic investigation on each affected endpoint before taking action
- D. Manually forwarding the alert to another team for verification

**Answer: A**

### Question: 10

In Cortex XSOAR, what is the key difference between scripts and jobs?  
Response:

- A. Scripts run on-demand or as part of playbooks, whereas jobs execute on a scheduled basis

- B. Scripts require manual execution, while jobs are fully automated
- C. Jobs only execute when Cortex XDR detects a new security threat
- D. Scripts store historical security incidents, whereas jobs do not

**Answer: A**

**Thank You for Trying Our Product**

**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**