

Palo Alto Networks XSIAM-Analyst

Palo Alto Networks XSIAM Analyst

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/xsiam-analyst>

Latest Version: 6.0

Question: 1

In the Identity Threat Detection and Response (ITDR) module, what does "compromised identity" typically indicate?

Response:

- A. Failed software update
- B. Unauthorized access or behavior from a known identity
- C. Missing antivirus signature
- D. USB device connection

Answer: B

Question: 2

An alert fires indicating lateral movement between endpoints. It was triggered after evaluating multiple unrelated activities, such as credential access and abnormal port scanning. What are likely characteristics of this alert?

(Choose two)

Response:

- A. Triggered by an IOC match
- B. Behaviorally inferred by a correlation rule
- C. Suggests a pre-configured playbook was executed
- D. Likely caused by a multi-stage correlation rule

Answer: B,D

Question: 3

You observe that a CVE is impacting multiple assets. How can you use ASM to investigate further? (Choose two)

Response:

- A. Review asset tags and status
- B. Trigger a Cortex data purge
- C. Validate attack surface rule hits
- D. Disable detection rules

Answer: A,C

Question: 4

An alert for malware propagation triggers an incident. The associated playbook isolates the endpoint and notifies the SOC team. What advantages does this approach provide?

(Choose two)

Response:

- A. Reduces mean time to respond (MTTR)
- B. Prevents SOC teams from seeing alert metadata
- C. Automates critical response actions
- D. Allows unrestricted user activity

Answer: A,C

Question: 5

Which option allows continuous monitoring and triage of evolving threats?

Response:

- A. Live terminal execution
- B. Threat intelligence API
- C. Attack Surface Threat Response Center
- D. Asset status logs

Answer: C

Question: 6

Which type of alert in Cortex XSIAM is primarily based on endpoint telemetry and behavior?

Response:

- A. IOC
- B. Correlation
- C. XDR Agent
- D. BIOC

Answer: D

Question: 7

You are hunting for endpoints that have recently executed PowerShell commands. Which two XQL query steps are appropriate?

Response:

- A. Use the xdm.process table
- B. Filter events by command-line arguments
- C. Query the xdm.asset table for policy info
- D. Export user reports from SIEM

Answer: A,B

Question: 8

An alert involves credential dumping. Reviewing the causality chain, you notice the following:

- lsass.exe is accessed by powershell.exe
- Prior to this, cmd.exe launched the PowerShell script

What can you infer?

Response:

- A. Scripted behavior likely launched manually
- B. There is an indicator of defense evasion
- C. It's a known benign service activity
- D. Possible credential access tactic

Answer: B,D

Question: 9

Which of the following actions is most appropriate in the Playground?

Response:

- A. Modify live alert data
- B. Simulate automation scripts without affecting real data
- C. Change alert severities globally
- D. Disable incident creation rules

Answer: B

Question: 10

You notice multiple endpoints reporting offline in XSIAM. Which actions would help confirm their operational status?

Response:

- A. Review recent heartbeat logs
- B. Perform a live terminal scan
- C. Ping the endpoint from the agent
- D. Check agent connection timestamps

Answer: A,D

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

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

Visit our website.

<https://examsempire.com/>