Vendor: Palo Alto Networks

Exam Code: XSIAM-Analyst

Exam Name: Palo Alto Networks XSIAM Analyst

Version: DEMO

QUESTION 1
Which type of task can be used to create a decision tree in a playbook?

A. Sub-playbook
B. Job
C. Standard
D. Conditional

Answer: D
Explanation:
Conditional tasks let you define multiple outcome branches based on evaluated expressions, enabling decision-tree logic within a playbook.

QUESTION 2
A Cortex XSIAM analyst is investigating a security incident involving a workstation after having deployed a Cortex XDR agent for 45 days. The incident details include the Cortex XDR Analytics Alert "Uncommon remote scheduled task creation."

Which response will mitigate the threat?

A. Revoke user access and conduct a user audit.
B. Allow list the processes to reduce alert noise.
C. Initiate the endpoint isolate action to contain the threat.
D. Prioritize blocking the source IP address to prevent further login attempts.

Answer: C
Explanation:
An “Uncommon remote scheduled task creation” suggests possible remote code execution or persistence. Isolating the affected endpoint immediately cuts it off from the network, stopping command-and-control or lateral movement while you investigate and remediate.

QUESTION 3
Which Cytool command will re-enable protection on an endpoint that has Cortex XDR agent protection paused?

A. `cytool security enable`
B. `cytool service start`
C. `cytool runtime start`
D. `cytool protect enable`

Answer: D
Explanation:
The `cytool protect enable` command re-enables protection modules (files, processes, registry, services) on an endpoint where Cortex XDR agent protection had been paused using cytool protect disable.

QUESTION 4
A Cortex XSIAM analyst is reading a blog that references an unfamiliar critical zero-day vulnerability. This vulnerability has been weaponized, and there is evidence that it is being exploited by threat actors targeting a customer's industry.

Where can the analyst go within Cortex XSIAM to learn more about this vulnerability and any potential impacts on the customer environment?

A. Threat Intel Management --> Sample Analysis
B. Attack Surface --> Threat Response Center
C. Attack Surface --> Attack Surface Rules
D. Threat Intel Management --> Indicator

Answer: B
Explanation:
The Threat Response Center centralizes emerging/zero-day vulnerability intelligence and correlates it with your environment, showing impact, affected assets, and recommended actions.

QUESTION 5
While investigating an alert, an analyst notices that a URL indicator has a related alert from a previous incident. The related alert has the same URL, but it resolved to a different IP address.

Which combination of two actions should the analyst take to resolve this issue? (Choose two.)

A. Enrich the IP address indicator associated with the previous alert.
B. Expire the URL indicator.
C. Remove the relationship between the URL and the older IP address.
D. Enrich the URL indicator.

Answer: CD
Explanation:
Removing the outdated URL-IP relationship clears the incorrect linkage, and enriching the URL indicator updates it with the current resolution and context so future alerts reflect the right association.

QUESTION 6
Which two actions will allow a security analyst to review updated commands from the core pack and interpret the results without altering the incident audit? (Choose two.)

A. Create a playbook with the commands and run it from within the War Room.
B. Run the core commands directly by typing them into the playground CLI.
C. Run the core commands directly from the Command and Scripts menu inside playground.
D. Run the core commands directly from the playground and invite other collaborators.

Answer: BC
Explanation:
Executing core pack commands in the Playground — either by typing them in the CLI or selecting them from Command & Scripts — lets you test and view results without writing anything to an incident's War Room audit trail.

QUESTION 7
Based on the artifact details in the image below, what can an analyst infer from the hexagon-shaped object with the exclamation mark (!) at the center?

A. The malicious artifact was injected.
B. The malware requires further analysis.
C. The WildFire verdict returned is "Low Confidence."
D. The artifact verdict has changed from a previous state to "Malware."

Answer: D
Explanation:
In Cortex XSIAM, the hexagon with an exclamation mark denotes a verdict change. Seeing it next to the artifact means its status was updated—now classified as Malware.

QUESTION 8
An analyst is responding to a critical incident involving a potential ransomware attack. The analyst immediately initiates full isolation on the compromised endpoint using Cortex XSIAM to prevent the malware from spreading across the network. However, the analyst now needs to collect additional forensic evidence from the isolated machine, including memory dumps and disk images, without reconnecting it to the network.

Which action will allow the analyst to collect the required forensic evidence while ensuring the endpoint remains fully isolated?

A. Using the management console to remotely run a predefined forensic playbook on the associated alert
B. Collecting the evidence manually through the agent by accessing the machine directly and running "Generate Support File"
C. Using the endpoint isolation feature to create a secure tunnel for evidence collection
D. Disabling full isolation temporarily to allow forensic tools to communicate with the endpoint

Answer: B
Explanation:
In situations where full isolation is enabled on an endpoint, all network communication is completely restricted. To ensure that the endpoint remains isolated while still obtaining forensic evidence such as memory dumps or disk images, the analyst needs to use manual collection via the agent directly on the machine. The "Generate Support File" feature within the agent allows analysts to locally gather detailed forensic data without breaking network isolation.

This manual method ensures the endpoint does not reconnect or communicate externally, maintaining strict isolation for security purposes.

"In endpoint isolation mode, network communication is completely blocked. Analysts should utilize the local 'Generate Support File' function on the agent to collect forensic data while maintaining full isolation."

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**