Latest XSIAM-Analyst Test Labs | New XSIAM-Analyst Dumps

P.S. Free & New XSIAM-Analyst dumps are available on Google Drive shared by Itcertking: https://drive.google.com/open?id=1-wMvOLkw1SAHYYvgJ7z13Uzu0E9Lz23u

Our company provides three different versions to choice for our customers. The software version of our XSIAM-Analyst exam question has a special function that this version can simulate test-taking conditions for customers. If you feel very nervous about exam, we think it is very necessary for you to use the software version of our XSIAM-Analyst Guide Torrent. By simulating actual test-taking conditions, we believe that you will relieve your nervousness before examination. So hurry to buy our XSIAM-Analyst test questions, it will be very helpful for you to pass your XSIAM-Analyst exam and get your certification.

Our products are definitely more reliable and excellent than other exam tool. What is more, the passing rate of our study materials is the highest in the market. There are thousands of customers have passed their exam and get the related certification. After that, all of their XSIAM-Analyst Exam torrents were purchase on our website. In fact, purchasing our XSIAM-Analyst actual test means you have been half success. Good decision is of great significance if you want to pass the XSIAM-Analyst exam for the first time.

>> Latest XSIAM-Analyst Test Labs <<

100% Pass Quiz 2026 XSIAM-Analyst - Latest Palo Alto Networks XSIAM Analyst Test Labs

Do you want to pass XSIAM-Analyst exam easily? XSIAM-Analyst exam training materials of Itcertking is a good choice, which covers all the content and answers about XSIAM-Analyst exam dumps you need to know. Then you can master the difficult points in a limited time, pass the XSIAM-Analyst Exam in one time, improve your professional value and stand more closely to success.

Palo Alto Networks XSIAM-Analyst Exam Syllabus Topics:

Topic	Details

Topic 1	- Data Analysis with XQL: This section of the exam measures the skills of Security Data Analysts and covers using the XSIAM Query Language (XQL) to analyze and correlate security data. It involves understanding Cortex Data Models, analyzing events through datasets, and interpreting XQL syntax, schema, and query options such as libraries and scheduled queries.
Topic 2	- Threat Intelligence Management and ASM: This section of the exam measures the skills of Threat Intelligence Analysts and focuses on handling and analyzing threat indicators and attack surface management (ASM). It includes importing and managing indicators, validating reputations and verdicts, creating prevention and detection rules, and monitoring asset inventories. Candidates are expected to use the Attack Surface Threat Response Center to identify and remediate threats effectively.
Topic 3	- Incident Handling and Response: This section of the exam measures the skills of Incident Response Analysts and covers managing the complete lifecycle of incidents. It involves explaining the incident creation process, reviewing and investigating evidence through forensics and identity threat detection, analyzing and responding to security events, and applying automated responses. The section also focuses on interpreting incident context data, differentiating between alert grouping and data stitching, and hunting for potential IOCs.
Topic 4	- Endpoint Security Management: This section of the exam measures the skills of Endpoint Security Administrators and focuses on validating endpoint configurations and monitoring activities. It includes managing endpoint profiles and policies, verifying agent status, and responding to endpoint alerts through live terminals, isolation, malware scans, and file retrieval processes.
Topic 5	- Automation and Playbooks: This section of the exam measures the skills of SOAR Engineers and focuses on leveraging automation within XSIAM. It includes using playbooks for automated incident response, identifying playbook components like tasks, sub-playbooks, and error handling, and understanding the purpose of the playground environment for testing and debugging automated workflows.

Palo Alto Networks XSIAM Analyst Sample Questions (Q136-Q141):

NEW QUESTION # 136
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

NEW QUESTION # 137
A Cortex XSIAM analyst in a SOC is reviewing an incident involving a workstation showing signs of a potential breach. The incident includes an alert from Cortex XDR Analytics Alert source "Remote service command execution from an uncommon source." As part of the incident handling process, the analyst must apply response actions to contain the threat effectively.
Which initial Cortex XDR agent response action should be taken to reduce attacker mobility on the network?

- A. Terminate Process: Stop the suspicious processes identified
- B. Remove Malicious File: Delete the malicious file detected
- C. Block IP Address: Prevent future connections to the IP from the workstation
- D. Isolate Endpoint: Prevent the endpoint from communicating with the network

Answer: D

Explanation:
The correct answer isA - Isolate Endpoint.
The most effective initial response to contain a breach and reduce attacker mobility is toisolate the endpoint.
This action ensures that the compromised machine can no longer communicate with the network or external systems, effectively cutting off lateral movement and exfiltration by attackers, while still allowing controlled response operations.
"Isolate Endpoint is the primary response action used to immediately contain a threat by severing all network communication, thus limiting attacker movement during active incidents." Document Reference:EDU-270c-10-lab-guide_02.docx (1).pdf Page:Page 40 (Incident Handling/SOC section)

NEW QUESTION # 138
Which Cytool command will re-enable protection on an endpoint that has Cortex XDR agent protection paused?

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

Answer: D

Explanation:
The correct answer isA - cytool security enable.
The commandcytool security enableis used tore-enableCortex XDR agent protection on an endpoint after it has been paused or disabled. This command restores all core security functions as per XDR agent configuration.
"Use the cytool security enable command to re-enable the Cortex XDR agent's protection if it has been paused on an endpoint." Document Reference:EDU-270c-10-lab-guide_02.docx (1).pdf Page:Page 13 (Agent Deployment and Configuration section)

NEW QUESTION # 139
While investigating an IOC, you want to validate its presence in the environment. What steps should you take? (Choose two)
Response:

- A. Search the IOC in the Cortex dataset
- B. Check the endpoint inventory
- C. Run threat intel reputation scan
- D. Use the XQL query builder

Answer: A,D

NEW QUESTION # 140
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 from the playground and invite other collaborators.
- C. Run the core commands directly from the Command and Scripts menu inside playground
- D. Run the core commands directly by typing them into the playground CLI.

Answer: C,D

Explanation:
Correct answers areBandD.
In Cortex XSIAM/XSOAR, the playground provides a safe environment for testing commands without modifying the incident audit log or impacting live incidents.
* Option B:Running commands from the "Command and Scripts" menu within the playground allows review and interpretation of command outputs safely and isolated from actual incidents.
* Option D:Typing commands directly into the playground CLI similarly enables secure review and interpretation of results without affecting the incident audit or live data.
Options A and C are incorrect because:

* Option A invites collaboration, potentially impacting visibility or causing accidental changes.
* Option C creates playbooks that execute directly within the War Room, thus interacting with real incidents.

NEW QUESTION # 141
......