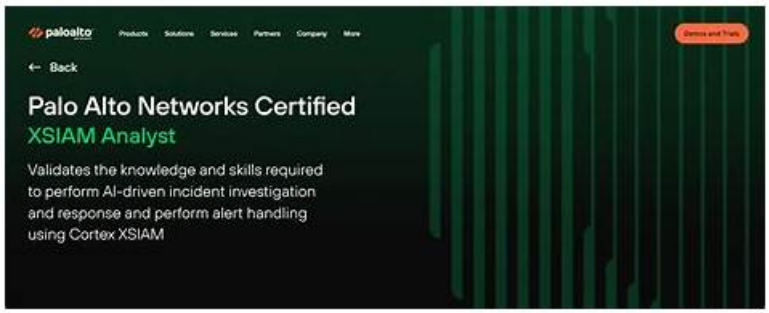
Pass Guaranteed Quiz Trustable Palo Alto Networks - XSIAM-Analyst Test Online



BTW, DOWNLOAD part of Dumpleader XSIAM-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1QVT34GSedcY7awuWPFuGZ4HhMMXycP6V

Our company Dumpleader abides by the industry norm all the time. By virtue of the help from professional experts, who are conversant with the regular exam questions of our latest XSIAM-Analyst real dumps. They can satisfy your knowledge-thirsty minds. And our XSIAM-Analyst Exam Quiz is quality guaranteed. By devoting ourselves to providing high-quality XSIAM-Analyst practice materials to our customers all these years we can guarantee all content is of the essential part to practice and remember.

Palo Alto Networks XSIAM-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.

>> XSIAM-Analyst Test Online <<

XSIAM-Analyst Book Free | XSIAM-Analyst Accurate Test

By years of diligent work, our experts have collected the frequent-tested knowledge into our XSIAM-Analyst practice materials for your reference. By resorting to our XSIAM-Analyst study guide, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our XSIAM-Analyst Actual Exam, the passing rate is 98-100 percent. So your chance of getting success will be increased greatly by our XSIAM-Analyst learning quiz.

Palo Alto Networks XSIAM Analyst Sample Questions (Q41-Q46):

NEW QUESTION # 41
What are sub-playbooks used for in Cortex XSIAM?
Response:

- A. To modularize common response actions
- B. To store user behavior profiles
- C. To assign playbooks to SOC analysts manually
- D. To act as backup playbooks during failure

Answer: A

NEW QUESTION # 42
In Cortex XSIAM, what initiates the execution of a playbook?
Response:

- A. SIEM log entry
- B. Query Library hit
- C. Alert correlation
- D. Incident trigger or manual run

Answer: D

NEW QUESTION # 43
Match each investigation objective with the most appropriate XDM datas
Objective
A) Investigate DNS abuse
B) Review endpoint alert activity
C) Analyze malware process spawning
D) Investigate suspicious file writes
Dataset
1. xdm.dns_query
2. xdm.endpoint_alert
3. xdm.process
4. xdm.file_event
Response:

- A. A-1, B-2, C-3, D-4
- B. A-1, B-3, C-2, D-4
- C. A-1, B-4, C-3, D-2
- D. A-4, B-2, C-3, D-1

Answer: A

NEW QUESTION # 44
A team wants to increase priority for alerts involving finance endpoints. Which methods would apply in Cortex XSIAM? (Choose two)
Response:

- A. Tag finance machines and update custom prioritization rule
- B. Define custom incident scoring rule based on device group
- C. Enable auto-remediation in playbooks
- D. Use user behavior analytics to override scores

Answer: A,B

NEW QUESTION # 45
Which of the following is NOT a task type in Cortex XSIAM playbooks?
Response:

- A. Automation script

- B. Reinforcement task
- C. Manual task
- D. Conditional task

Answer: B

NEW QUESTION # 46
.....

As we all know that if we get a certificate for the exam, we will have more advantages in the job market. We have XSIAM-Analyst study guide for you to get the certificate quickly. Besides, we are pass guarantee, if you indeed fail the exam, we will be money back guarantee. XSIAM-Analyst Study Guide of us obtain many good feedbacks from our customers. Free demo of XSIAM-Analyst exam dumps are provided by us, you can have a try before you buy them, so that you can know the mode of the XSIAM-Analyst learning materials.

id=1QVT34GSedcY7awuWPFuGZ4HhMMXycP6V