Choose Palo Alto Networks XDR-Analyst Exam Questions for Successful Preparation

We will refund your money if you fail to pass the exam after buying XDR-Analyst study materials. If you choose us, we will ensure you pass the exam. And we are pass guaranteed and money back guaranteed. Besides, XDR-Analyst study materials of us will help you pass the exam just one time. With professional experts to compile the XDR-Analyst Exam Dumps, they are high- quality. And we also have online and offline chat service stuff, who possess the professional knowledge about the XDR-Analyst study materials, and if you have any questions, just contact us, we will give you reply as quickly as possible.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques.
Topic 2	• Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights.
Topic 3	• Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
Topic 4	• Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions.

>> XDR-Analyst Practice Test Fee <<

100% Pass 2026 Palo Alto Networks XDR-Analyst: Palo Alto Networks XDR Analyst Accurate Practice Test Fee

Whether for a student or an office worker, obtaining XDR-Analyst certificate can greatly enhance the individual's competitiveness in the future career. Try our XDR-Analyst study materials, which are revised by hundreds of experts according to the changes in the syllabus and the latest developments in theory and practice. Once you choose XDR-Analyst training dumps, passing the exam one time is no longer a dream.

Palo Alto Networks XDR Analyst Sample Questions (Q66-Q71):

NEW QUESTION # 66
What license would be required for ingesting external logs from various vendors?

- A. Cortex XDR Vendor Agnostic Pro
- B. Cortex XDR Pro per Endpoint
- C. Cortex XDR Pro per TB
- D. Cortex XDR Cloud per Host

Answer: C

Explanation:
To ingest external logs from various vendors, you need a Cortex XDR Pro per TB license. This license allows you to collect and analyze logs from Palo Alto Networks and third-party sources, such as firewalls, proxies, endpoints, cloud services, and more. You can use the Log Forwarding app to forward logs from the Logging Service to an external syslog receiver. The Cortex XDR Pro per Endpoint license only supports logs from Cortex XDR agents installed on endpoints. The Cortex XDR Vendor Agnostic Pro and Cortex XDR Cloud per Host licenses do not exist. Reference:
Features by Cortex XDR License Type
Log Forwarding App for Cortex XDR Analytics
SaaS Log Collection

NEW QUESTION # 67
What is the standard installation disk space recommended to install a Broker VM?

- A. 512GB disk space
- B. 256GB disk space
- C. 2GB disk space
- D. 1GB disk space

Answer: B

Explanation:
The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location. The system requirements for the Broker VM are as follows:
CPU: 4 cores
RAM: 8 GB
Disk space: 256 GB
Network: Internet access and connectivity to all Cortex XDR agents
The disk space requirement is based on the number of agents and the frequency of content updates. The Broker VM stores the content updates locally and distributes them to the agents. The disk space also depends on the retention period of the content updates, which can be configured in the Broker VM settings. The default retention period is 30 days.
Reference:
Broker VM for Cortex XDR
PCDRA Study Guide

NEW QUESTION # 68
With a Cortex XDR Prevent license, which objects are considered to be sensors?

- A. Palo Alto Networks Next-Generation Firewalls
- B. Cortex XDR agents
- C. Third-Party security devices
- D. Syslog servers

Answer: B

Explanation:
The objects that are considered to be sensors with a Cortex XDR Prevent license are Cortex XDR agents and Palo Alto Networks Next-Generation Firewalls. These are the two sources of data that Cortex XDR can collect and analyze for threat detection and response. Cortex XDR agents are software components that run on endpoints, such as Windows, Linux, and Mac devices, and provide protection against malware, exploits, and fileless attacks. Cortex XDR agents also collect and send endpoint data, such as process activity, network traffic, registry changes, and user actions, to the Cortex Data Lake for analysis and correlation. Palo Alto Networks Next-Generation Firewalls are network security devices that provide visibility and control over network traffic, and enforce security policies based on applications, users, and content. Next-Generation Firewalls also collect and send network data, such as firewall logs, DNS logs, HTTP headers, and WildFire verdicts, to the Cortex Data Lake for analysis and correlation. By integrating data from both Cortex XDR agents and Next-Generation Firewalls, Cortex XDR can provide a comprehensive view of the attack surface and detect threats across the network and endpoint layers. Reference:
Cortex XDR Prevent License
Cortex XDR Agent Features
Next-Generation Firewall Features

NEW QUESTION # 69
You can star security events in which two ways? (Choose two.)

- A. Create an Incident-starring configuration.
- B. Manually star an alert.
- C. Create an alert-starring configuration.
- D. Manually star an Incident.

Answer: B,D

Explanation:
You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you prioritize and track the events that are most important to you. You can also filter and sort the events by their star status in the Cortex XDR console.
To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again.
To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed.
Reference:
Star Security Events
Create an Alert Starring Configuration
Create an Incident Starring Configuration

NEW QUESTION # 70
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically kill the processes involved in malicious activity.
- B. Automatically close the connections involved in malicious traffic.
- C. Automatically block the IP addresses involved in malicious traffic.
- D. Automatically terminate the threads involved in malicious activity.

Answer: A,C

NEW QUESTION # 71

......

All these advantages will be available after passing the Palo Alto Networks XDR Analyst XDR-Analyst certification exam which is not easy to pass. However, the complete XDR-Analyst test preparation and proper planning can enable you to crack the Palo Alto Networks XDR-Analyst exam easily. For the complete and comprehensive XDR-Analyst exam preparation, you can trust Palo Alto Networks XDR-Analyst PDF Questions and practice tests. The Palo Alto Networks is one of the leading platforms that are committed to ace the Palo Alto Networks XDR Analyst XDR-Analyst Exam Preparation with the Palo Alto Networks XDR-Analyst valid dumps. The Palo Alto Networks XDR-Analyst practice questions are the real XDR-Analyst exam questions that are verified by experience and qualified Palo Alto Networks XDR-Analyst exam experts.

XDR-Analyst Reliable Test Duration: https://www.dumpexam.com/XDR-Analyst-valid-torrent.html

- Real XDR-Analyst Exam Questions □ XDR-Analyst Questions Answers □ XDR-Analyst Exam Preparation □ Search for □ XDR-Analyst □ on （ www.testkingpass.com ） immediately to obtain a free download □XDR-Analyst Exam Objectives Pdf
- XDR-Analyst Study Guide Practice Materials and XDR-Analyst Actual Dumps and Torrent - Pdfvce □ Open website □ www.pdfvce.com □ and search for □ XDR-Analyst □ for free download □Reliable XDR-Analyst Test Pass4sure
- Reliable Palo Alto Networks XDR-Analyst Practice Test Fee With Interarctive Test Engine - Trustable XDR-Analyst Reliable Test Duration □ Simply search for ➥ XDR-Analyst □ for free download on ➽ www.easy4engine.com □ □ □Latest XDR-Analyst Exam Question
- Real XDR-Analyst Exam Questions □ XDR-Analyst Braindumps Torrent □ XDR-Analyst Pass Guide □ Open ➽ www.pdfvce.com □ and search for [XDR-Analyst] to download exam materials for free □Latest XDR-Analyst Study Plan
- XDR-Analyst Pass Guide □ XDR-Analyst Latest Exam Fee □ Valid XDR-Analyst Test Topics □ Easily obtain free download of □ XDR-Analyst □ by searching on ▶ www.prepawayete.com ◀ □XDR-Analyst Braindumps Torrent
- XDR-Analyst Exam Preparation □ Latest XDR-Analyst Study Plan □ Latest XDR-Analyst Study Plan □ Open ➠ www.pdfvce.com □ and search for [XDR-Analyst] to download exam materials for free □Reliable XDR-Analyst Test Pass4sure
- Palo Alto Networks XDR-Analyst Exam Questions: Attain Your Professional Career Goals [2026] □ Search on ▷ www.prep4sures.top ◁ for ➡ XDR-Analyst □□□ to obtain exam materials for free download □XDR-Analyst Accurate Prep Material
- Palo Alto Networks XDR-Analyst Practice Test Fee: Palo Alto Networks XDR Analyst - Pdfvce Brings the best Reliable Test Duration with One Year Free Updates □ Search for { XDR-Analyst } and obtain a free download on ⇒ www.pdfvce.com ⇐ □Reliable XDR-Analyst Test Pass4sure
- XDR-Analyst Practice Test Fee 100% Pass | Reliable XDR-Analyst: Palo Alto Networks XDR Analyst 100% Pass □ Search for □ XDR-Analyst □ and easily obtain a free download on ➤ www.pdfdumps.com □ □Reliable XDR-Analyst Test Pass4sure
- XDR-Analyst Latest Exam Fee □ Dumps XDR-Analyst Collection □ Valid Dumps XDR-Analyst Sheet □ Copy URL { www.pdfvce.com } open and search for □ XDR-Analyst □ to download for free □Test XDR-Analyst Online
- XDR-Analyst Pass Guide □ XDR-Analyst Questions Answers □ New XDR-Analyst Test Pass4sure □ Go to website 「 www.pass4test.com 」 open and search for ➡ XDR-Analyst □□□ to download for free □Valid Dumps XDR-Analyst Sheet
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 99tt2.ml30.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes