The Palo Alto Networks XDR-Analyst Web-Based Practice Exam

2026 Latest Prep4sureGuide XDR-Analyst PDF Dumps and XDR-Analyst Exam Engine Free Share: https://drive.google.com/open?id=1iDsOBsydLyABxcUNr5cVk7wNhtfhAsuV

Well preparation is half done, so choosing good XDR-Analyst training materials is the key of clear exam in your first try with less time and efforts. Our website offers you the latest preparation materials for the XDR-Analyst real exam and the study guide for your review. There are three versions according to your study habit and you can practice our XDR-Analyst Dumps PDF with our test engine that help you get used to the atmosphere of the formal test.

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	• Endpoint Security Management:
Topic 3	• 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.
Topic 4	• 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 5	• This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.

>> XDR-Analyst Exam Cram Review <<

Online Palo Alto Networks XDR-Analyst Lab Simulation & Practice XDR-Analyst Mock

Are you still distressed that you are young learner of XDR-Analyst exam prep? From now on, Prep4sureGuide will solve all your worries about the XDR-Analyst test. The textbooks of XDR-Analyst test questions contain different perspective materials. Even if you are young learners, you can master XDR-Analyst Test Questions easily. Having it, you will have the key to pass XDR-Analyst exam and will have unprecedented confidence. So what are you waiting for?

Palo Alto Networks XDR Analyst Sample Questions (Q24-Q29):

NEW QUESTION # 24
What is the purpose of the Cortex Data Lake?

- A. a local storage facility where your logs and alert data can be aggregated
- B. the interface between firewalls and the Cortex XDR agents
- C. a cloud-based storage facility where your firewall logs are stored
- D. the workspace for your Cortex XDR agents to detonate potential malware files

Answer: C

Explanation:
The purpose of the Cortex Data Lake is to provide a cloud-based storage facility where your firewall logs are stored. Cortex Data Lake is a service that collects, transforms, and integrates your enterprise's security data to enable Palo Alto Networks solutions. It powers AI and machine learning, detection accuracy, and app and service innovation. Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure, including your next-generation firewalls, Prisma Access, and Cortex XDR. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is available in multiple regions and supports data residency and privacy requirements. Reference:
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake, the technology behind Cortex XDR - Palo Alto Networks CORTEX DATA LAKE - Palo Alto Networks
Sizing for Cortex Data Lake Storage - Palo Alto Networks

NEW QUESTION # 25
Which of the following paths will successfully activate Remediation Suggestions?

- A. Alerts Table > Right-click on an alert > Remediation Suggestions
- B. Causality View > Actions > Remediation Suggestions
- C. Alerts Table > Right-click on a process node > Remediation Suggestions
- D. Incident View > Actions > Remediation Suggestions

Answer: B

Explanation:
Remediation Suggestions is a feature of Cortex XDR that provides you with recommended actions to remediate the root cause and impact of an incident. Remediation Suggestions are based on the analysis of the causality chain, the behavior of the malicious files or processes, and the best practices for incident response. Remediation Suggestions can help you to quickly and effectively contain and resolve an incident, as well as prevent future recurrence.
To activate Remediation Suggestions, you need to follow these steps:
In the Cortex XDR management console, go to Incidents and select an incident that you want to remediate.
Click Causality View to see the graphical representation of the causality chain of the incident.
Click Actions and select Remediation Suggestions. This will open a new window that shows the suggested actions for each node in the causality chain.
Review the suggested actions and select the ones that you want to apply. You can also edit or delete the suggested actions, or add your own custom actions.
Click Apply to execute the selected actions on the affected endpoints. You can also schedule the actions to run at a later time or date.

Reference:
Remediate Changes from Malicious Activity: This document explains how to use Remediation Suggestions to remediate the root cause and impact of an incident.
Causality View: This document describes how to use Causality View to investigate the causality chain of an incident.

NEW QUESTION # 26
In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

- A. Click the star in the widget
- B. Create a custom XQL widget
- C. Create a custom report and filter on starred incidents
- D. This is not currently supported

Answer: A

Explanation:
To filter the display to only show incidents that were "starred", you need to click the star in the widget. This will apply a filter that shows only the incidents that contain a starred alert, which is an alert that matches a specific condition that you define in the incident starring configuration. You can use the incident starring feature to prioritize and focus on the most important or relevant incidents in your environment1.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Create a custom XQL widget: This is not the correct answer. Creating a custom XQL widget is not necessary to filter the display to only show starred incidents. A custom XQL widget is a widget that you create by using the XQL query language to define the data source and the visualization type. You can use custom XQL widgets to create your own dashboards or reports, but they are not required for filtering incidents by stars2.
B . This is not currently supported: This is not the correct answer. Filtering the display to only show starred incidents is currently supported by Cortex XDR. You can use the star icon in the widget to apply this filter, or you can use the Filter Builder to create a custom filter based on the Starred field1.
C . Create a custom report and filter on starred incidents: This is not the correct answer. Creating a custom report and filtering on starred incidents is not the only way to filter the display to only show starred incidents. A custom report is a report that you create by using the Report Builder to define the data source, the layout, and the schedule. You can use custom reports to generate and share periodic reports on your Cortex XDR data, but they are not the only option for filtering incidents by stars3.
In conclusion, clicking the star in the widget is the simplest and easiest way to filter the display to only show incidents that were "starred". By using this feature, you can quickly identify and focus on the most critical or relevant incidents in your environment.
Reference:
Filter Incidents by Stars
Create a Custom XQL Widget
Create a Custom Report

NEW QUESTION # 27
What license would be required for ingesting external logs from various vendors?

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

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 # 28
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

- A. WebSocket
- B. TCP, over port 80
- C. UDP and a random port
- D. NetBIOS over TCP

Answer: A

Explanation:
Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. Reference:
Initiate a Live Terminal Session
WebSocket

NEW QUESTION # 29
.....

Our XDR-Analyst exam questions are unlike other study materials that are available on the market, XDR-Analyst guide quiz specially proposed different versions to allow you to learn not only on paper, but also to use mobile phones to learn. And if you buy the value pack, you have all of the three versions, the price is quite preferential and you can enjoy all of the study experiences. This means you can XDR-Analyst Practice Engine anytime and anyplace for the convenience these three versions bring.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bookmarkilo.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, socialdosa.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Download part of Prep4sureGuide XDR-Analyst dumps for free: https://drive.google.com/open?id=1iDsOBsydLyABxcUNr5cVk7wNhtfhAsuV