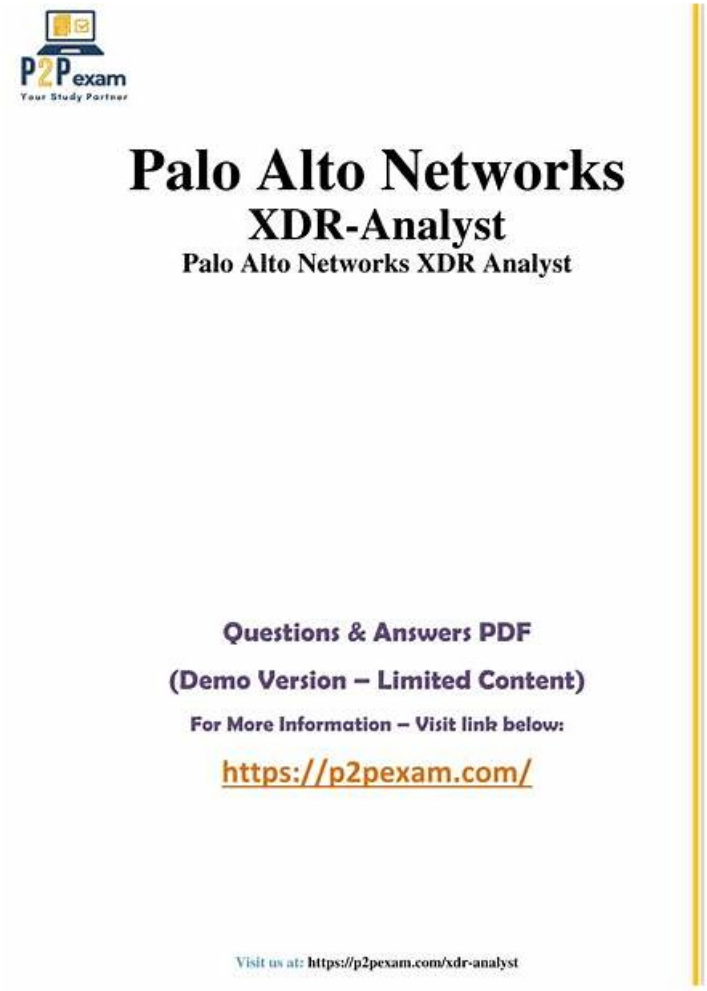
Purchase Palo Alto Networks XDR-Analyst Exam Questions Today for Hassle-Free Preparation



As we all know, the world does not have two identical leaves. People's tastes also vary a lot. So we have tried our best to develop the three packages of our XDR-Analyst exam braindumps for you to choose. Now we have free demo of the XDR-Analyst study materials exactly according to the three packages on the website for you to download before you pay for the XDR-Analyst Practice Engine, and the free demos are a small part of the questions and answers. You can check the quality and validity by them.

If you want to know the latest information for the exam timely, you can choose us, we can do that for you. We offer you free update for one year for XDR-Analyst learning materials, so that you can obtain the latest information for the exam. Our system will send you the latest version automatically, and you just need to examine your email for the latest version. In addition, XDR-Analyst Exam Materials are high-quality, and you can improve your efficiency by using them. We have online and offline service, and if you have any questions for XDR-Analyst exam braindumps, you can contact us, and we will give you reply as quickly as we can.

>> XDR-Analyst Pass4sure Pass Guide <<

Palo Alto Networks XDR-Analyst Trustworthy Pdf & XDR-Analyst Test Questions Fee

The best news is that during the whole year after purchasing, you will get the latest version of our XDR-Analyst exam prep study materials for free, since as soon as we have compiled a new version of the XDR-Analyst study materials, our company will send the latest one of our XDR-Analyst study materials to your email immediately. Therefore, we can assure that you will miss nothing needed for the XDR-Analyst Exam. What's more, the latest version of our XDR-Analyst study materials will be a good way for you to broaden your horizons as well as improve your skills.

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	• 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	• 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.

Palo Alto Networks XDR Analyst Sample Questions (Q15-Q20):

NEW QUESTION # 15
Which statement is true based on the following Agent Auto Upgrade widget?

- A. There are a total of 689 Up To Date agents.
- B. Agent Auto Upgrade was enabled but not on all endpoints.
- C. Agent Auto Upgrade has not been enabled.
- D. There are more agents in Pending status than In Progress status.

Answer: B

Explanation:
The Agent Auto Upgrade widget shows the status of the agent auto upgrade feature on the endpoints. The widget displays the number of agents that are up to date, in progress, pending, failed, and not configured. In this case, the widget shows that there are 450 agents that are up to date, 78 in progress, 15 pending, 18 failed, and 128 not configured. This means that the agent auto upgrade feature was enabled but not on all endpoints. Reference:
Cortex XDR Agent Auto Upgrade
PCDRA Study Guide

NEW QUESTION # 16
What is the difference between presets and datasets in XQL?

- A. A dataset is a Cortex data lake data source only; presets are built-in data source.
- B. A dataset is a database; presets is a field.
- C. A dataset is a built-in or third-party source; presets group XDR data fields.
- D. A dataset is a third-party data source; presets are built-in data source.

Answer: C

Explanation:
The difference between presets and datasets in XQL is that a dataset is a built-in or third-party data source, while a preset is a group of XDR data fields. A dataset is a collection of data that you can query and analyze using XQL. A dataset can be a Cortex data lake data source, such as endpoints, alerts, incidents, or network flows, or a third-party data source, such as AWS CloudTrail, Azure Activity Logs, or Google Cloud Audit Logs. A preset is a predefined set of XDR data fields that are relevant for a specific use case, such as process execution, file operations, or network activity. A preset can help you simplify and standardize your XQL queries by selecting the most important fields for your analysis. You can use presets with any Cortex data lake data source, but not with third-party data sources. Reference:

Datasets and Presets
XQL Language Reference

NEW QUESTION # 17
Which of the following policy exceptions applies to the following description?
'An exception allowing specific PHP files'

- A. Process exception
- B. Support exception
- C. Behavioral threat protection rule exception
- D. Local file threat examination exception

Answer: D

Explanation:
The policy exception that applies to the following description is B, local file threat examination exception. A local file threat examination exception is an exception that allows you to exclude specific files or folders from being scanned by the Cortex XDR agent for malware or threats. You can use this exception to prevent false positives, performance issues, or compatibility problems with legitimate files or applications. You can define the local file threat examination exception by file name, file path, file hash, or digital signer. For example, you can create a local file threat examination exception for specific PHP files by entering their file names or paths in the exception configuration. Reference:
Local File Threat Examination Exceptions
Create a Local File Threat Examination Exception

NEW QUESTION # 18
How can you pivot within a row to Causality view and Timeline views for further investigate?

- A. You can't pivot within a row to Causality view and Timeline views
- B. Using the Open Card Only
- C. Using Open Timeline Actions Only
- D. Using the Open Card and Open Timeline actions respectively

Answer: D

Explanation:
To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident. Reference:
Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

NEW QUESTION # 19
What is the Wildfire analysis file size limit for Windows PE files?

- A. 100MB
- B. 500MB
- C. 1GB
- D. No Limit

Answer: A

Explanation:
The Wildfire analysis file size limit for Windows PE files is 100MB. Windows PE files are executable files that run on the Windows operating system, such as .exe, .dll, .sys, or .scr files. Wildfire is a cloud-based service that analyzes files and URLs for malicious behavior and generates signatures and protections for them. Wildfire can analyze various file types, such as PE, APK, PDF, MS Office, and others, but each file type has a different file size limit. The file size limit determines the maximum size of the file that can be

uploaded or forwarded to Wildfire for analysis. If the file size exceeds the limit, Wildfire will not analyze the file and will return an error message.
According to the Wildfire documentation1, the file size limit for Windows PE files is 100MB. This means that any PE file that is larger than 100MB will not be analyzed by Wildfire. However, the firewall can still apply other security features, such as antivirus, anti-spyware, vulnerability protection, and file blocking, to the PE file based on the security policy settings. The firewall can also perform local analysis on the PE file using the Cortex XDR agent, which uses machine learning models to assess the file and assign it a verdict2.
Reference:
WildFire File Size Limits: This document provides the file size limits for different file types that can be analyzed by Wildfire.
Local Analysis: This document explains how the Cortex XDR agent performs local analysis on files that cannot be sent to Wildfire for analysis.

NEW QUESTION # 20
.....