XDR-Analyst Latest Test Guide | Trustworthy XDR-Analyst Practice

A free trial of the product allows users to test the material before buying. These different formats allow XDR-Analyst exam aspirants to practice using their preferred method. The support offered by the PassTorrent is another significant advantage for applicants. The PassTorrent XDR-Analyst provides 24/7 support for guidance of users. Our team of professionals is highly qualified and have years of experience in the industry. They are available to answer any Palo Alto Networks XDR-Analyst Questions that customers may have. The support team is always available to help applicants use the product.

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

>> XDR-Analyst Latest Test Guide <<

Trustworthy Palo Alto Networks XDR-Analyst Practice, XDR-Analyst Test Question

Our passing rate is 99% and our product boosts high hit rate. Our XDR-Analyst test torrents are compiled by professionals and the answers and the questions we provide are based on the real exam. The content of our XDR-Analyst exam questions is simple to be understood and mastered. To let you get well preparation for the exam, our software provides the function to stimulate the real exam and the timing function to help you adjust the speed. Based on those merits of our XDR-Analyst Guide Torrent you can pass the exam with high possibility.

Palo Alto Networks XDR Analyst Sample Questions (Q50-Q55):

NEW QUESTION # 50
What does the following output tell us?

- A. Host shpapy_win10 had the most vulnerabilities.
- B. This is an actual output of the Top 10 hosts with the most malware.
- C. There is one informational severity alert.
- D. There is one low severity incident.

Answer: B

Explanation:
The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more .
Reference:
Use the ACC to Analyze Network Activity
Top 10 Hosts with the Most Malware

NEW QUESTION # 51
In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

- A. Service Now
- B. Salesforce
- C. Slack
- D. Jira

Answer: C

Explanation:
Cortex XDR allows you to schedule reports and forward them to Slack, a cloud-based collaboration platform. You can configure the Slack channel, frequency, and recipients of the scheduled reports. You can also view the report history and status in the Cortex XDR management console. Reference:
Scheduled Queries: This document explains how to create, edit, and manage scheduled queries and reports in Cortex XDR.
Forward Scheduled Reports to Slack: This document provides the steps to configure Slack integration and forward scheduled reports to a Slack channel.

NEW QUESTION # 52
You can star security events in which two ways? (Choose two.)

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

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

Answer: A,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 # 53
The Cortex XDR console has triggered an incident, blocking a vitally important piece of software in your organization that is known to be benign. Which of the following options would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization?

- A. Create an endpoint-specific exception.
- B. Create a global inclusion.
- C. Create an individual alert exclusion.
- D. Create a global exception.

Answer: D

Explanation:
A global exception is a rule that allows you to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR. A global exception applies to all endpoints in your organization that are protected by Cortex XDR. Creating a global exception for a vitally important piece of software that is known to be benign would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization.
To create a global exception, you need to follow these steps:
In the Cortex XDR management console, go to Policy Management > Exceptions and click Add Exception.
Select the Global Exception option and click Next.
Enter a name and description for the exception and click Next.
Select the type of exception you want to create, such as file, process, or behavior, and click Next.
Specify the criteria for the exception, such as file name, hash, path, process name, command line, or behavior name, and click Next.
Review the summary of the exception and click Finish.
Reference:
Create Global Exceptions: This document explains how to create global exceptions to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR.
Exceptions Overview: This document provides an overview of exceptions and how they can be used to fine-tune the Cortex XDR security policy.

NEW QUESTION # 54
Which of the following Live Terminal options are available for Android systems?

- A. Run APK scripts.
- B. Stop an app.
- C. Live Terminal is not supported.
- D. Run Android commands.

Answer: D

Explanation:
Cortex XDR supports Live Terminal for Android systems, which allows you to remotely access and manage Android endpoints using a command-line interface. You can use Live Terminal to run Android commands, such as adb shell, adb logcat, adb install, and adb uninstall. You can also use Live Terminal to view and modify files, directories, and permissions on the Android endpoints. Live Terminal for Android systems does not support stopping an app or running APK scripts. Reference:
Cortex XDR documentation portal
Initiate a Live Terminal Session
Live Terminal Commands

NEW QUESTION # 55
.....

Here, the PassTorrent empathizes with them for the extreme frustration they undergo due to not finding updated and actual Palo Alto Networks XDR-Analyst exam dumps. It helps them by providing the exceptional Palo Alto Networks XDR-Analyst Questions to get the prestigious Palo Alto Networks XDR-Analyst certificate.