Try Test4Sure Palo Alto Networks XDR-Analyst Practice Test Software

Firstly, our company always feedbacks our candidates with highly-qualified XDR-Analyst study guide and technical excellence and continuously developing the most professional XDR-Analyst exam materials. Secondly, our XDR-Analyst study materials persist in creating a modern service oriented system and strive for providing more preferential activities for your convenience. Come and buy our XDR-Analyst Exam Materials, you will get more than you can imagine!

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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 Exam Guide <<

Reliable XDR-Analyst Cram Materials & Exam XDR-Analyst Question

The time and energy are all very important for the office workers. In order to get the XDR-Analyst certification with the less time and energy investment, you need a useful and valid XDR-Analyst study material for your preparation. XDR-Analyst free download pdf will be the right material you find. The comprehensive contents of XDR-Analyst practice torrent can satisfied your needs and help you solve the problem in the actual test easily. Now, choose our XDR-Analyst study practice, you will get high scores.

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

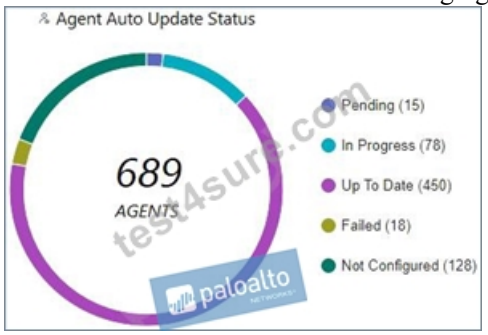
NEW QUESTION # 41
When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

- A. Remediation Automation
- B. Remediation Suggestions
- C. Machine Remediation
- D. Automatic Remediation

Answer: B

Explanation:
When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. Reference:
Remediation Suggestions
Apply Remediation Suggestions

NEW QUESTION # 42
Which statement is true based on the following Agent Auto Upgrade widget?



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

Answer: C

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 # 43
What is the difference between presets and datasets in XQL?

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

Answer: B

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 # 44
In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

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

Answer: B

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 # 45
What is the outcome of creating and implementing an alert exclusion?

- A. The Cortex XDR agent will not create an alert for this event in the future.
- B. The Cortex XDR console will hide those alerts.
- C. The Cortex XDR console will delete those alerts and block ingestion of them in the future.
- D. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

Answer: B

Explanation:
The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint. Therefore, the correct answer is B, the Cortex XDR console will hide those alerts12 Reference:
Alert Exclusions
Create an Alert Exclusion Policy

NEW QUESTION # 46
.....

Many candidates like APP test engine of XDR-Analyst exam braindumps because it seem very powerful. If you are interested in this version, you can purchase it. This version provides only the questions and answers of XDR-Analyst exam braindumps but also some functions easy to practice and master. It can be used on any electronic products if only it can open the browser such as Mobile Phone, Ipad and others. If you always have some fear for the real test or can't control the time to finish your test, APP test engine of Palo Alto Networks XDR-Analyst Exam Braindumps can set timed test and simulate the real test scene for your practice.

- Palo Alto Networks certification XDR-Analyst exam best training materials □ Download ⇛ XDR-Analyst ⇚ for free by simply entering □ www.pdfvce.com □ website □Reliable XDR-Analyst Braindumps Sheet
- XDR-Analyst Hot Questions □ New XDR-Analyst Exam Format □ Braindump XDR-Analyst Pdf □ Immediately open （ www.examcollectionpass.com ） and search for 【 XDR-Analyst 】 to obtain a free download □XDR-Analyst Valid Dumps Questions
- theatibyeinstitute.org, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, course.azizafkar.com, www.stes.tyc.edu.tw, pixabay.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes