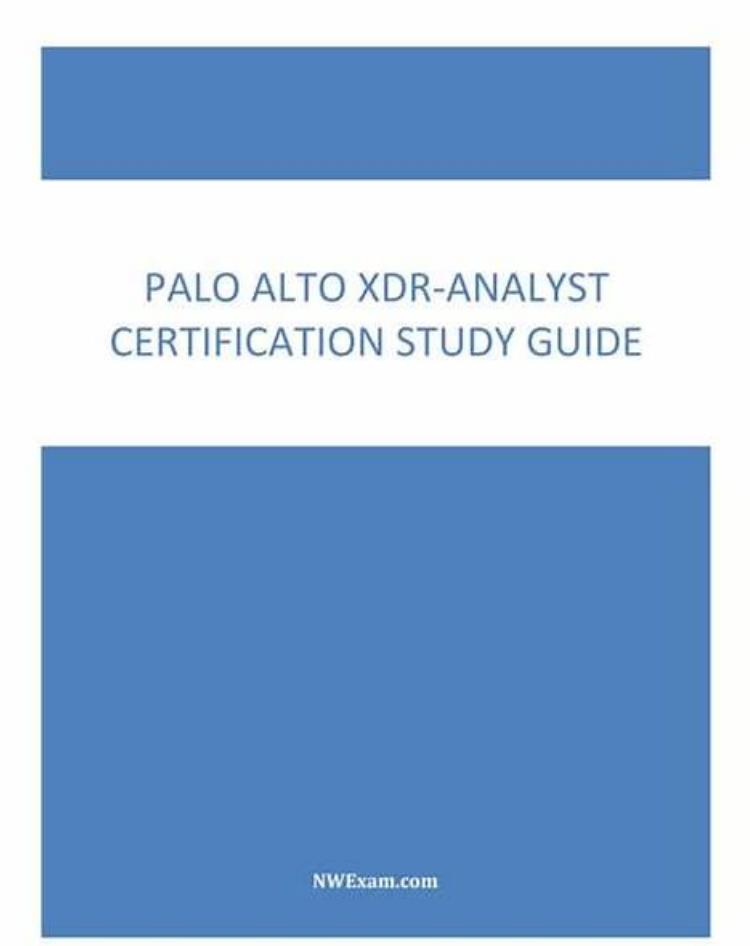
Pass Guaranteed Palo Alto Networks - Authoritative XDR-Analyst - Study Palo Alto Networks XDR Analyst Tool



If you use the trial version of our XDR-Analyst study materials, you will find that our products are very useful for you to pass your exam and get the certification. Though the trail version of our XDR-Analyst learning guide only contains a small part of the exam questions and answers, but it shows the quality and validity. If you buy our XDR-Analyst Exam Questions, we can promise that you will pass the exam for sure and gain the according the certification.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Endpoint Security Management:
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	• 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	• This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
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.

100% Pass Palo Alto Networks XDR-Analyst - Palo Alto Networks XDR Analyst First-grade Study Tool

PassTorrent provides proprietary preparation guides for the certification exam offered by the XDR-Analyst exam dumps. In addition to containing numerous questions similar to the XDR-Analyst Exam, the Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions are a great way to prepare for the Palo Alto Networks XDR-Analyst exam dumps.

Palo Alto Networks XDR Analyst Sample Questions (Q14-Q19):

NEW QUESTION # 14
When creating a BIOC rule, which XQL query can be used?

- A. dataset = xdr_data
  | filter event_type = PROCESS and
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- B. dataset = xdr_data
  | filter event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- C. dataset = xdr_data
  | filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
  | fields action_process_image
- D. dataset = xdr_data
  | filter event_behavior = true
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Answer: A

Explanation:
A BIOC rule is a custom detection rule that uses the Cortex Query Language (XQL) to define the behavior or actions that indicate a potential threat. A BIOC rule can use the xdr_data and cloud_audit_log datasets and presets for these datasets. A BIOC rule can also use the filter stage, alter stage, and functions without any aggregations in the XQL query. The query must return a single field named action_process_image, which is the process image name of the suspicious process. The query must also include the event_type and event_sub_type fields in the filter stage to specify the type and sub-type of the event that triggers the rule.
Option B is the correct answer because it meets all the requirements for a valid BIOC rule query. It uses the xdr_data dataset, the filter stage, the event_type and event_sub_type fields, and the action_process_image_name field with a regular expression to match any process image name that ends with .pdf.exe or .docx.exe, which are common indicators of malicious files.
Option A is incorrect because it does not include the event_type field in the filter stage, which is mandatory for a BIOC rule query.
Option C is incorrect because it does not include the event_type and event_sub_type fields in the filter stage, and it uses the fields stage, which is not supported for a BIOC rule query. It also returns the action_process_image field instead of the action_process_image_name field, which is the expected output for a BIOC rule query.
Option D is incorrect because it uses the event_behavior field, which is not supported for a BIOC rule query. It also does not include the event_type field in the filter stage, and it uses the event_sub_type field incorrectly. The event_sub_type field should be equal to PROCESS_START, not true.
Reference:
Working with BIOCs
Cortex Query Language (XQL) Reference

NEW QUESTION # 15
What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

- A. Keylogger
- B. Ransomware
- C. Worm
- D. Rootkit

Answer: B

Explanation:
The kind of malware that uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim is ransomware. Ransomware is a type of malware that encrypts the victim's files or blocks access to their system, and then demands a ransom for the decryption key or the restoration of access. Ransomware can also threaten to expose or delete the victim's data if the ransom is not paid. Ransomware can cause significant damage and disruption to individuals, businesses, and organizations, and can be difficult to remove or recover from. Some examples of ransomware are CryptoLocker, WannaCry, Ryuk, and REvil.
Reference:
12 Types of Malware + Examples That You Should Know - CrowdStrike
What is Malware? Malware Definition, Types and Protection
12+ Types of Malware Explained with Examples (Complete List)

NEW QUESTION # 16
Can you disable the ability to use the Live Terminal feature in Cortex XDR?

- A. No, a separate installer package without Live Terminal is required.
- B. No, it is a required feature of the agent.
- C. Yes, via Agent Settings Profile.
- D. Yes, via the Cortex XDR console or with an installation switch.

Answer: C

Explanation:
The Live Terminal feature in Cortex XDR allows you to initiate a remote connection to an endpoint and perform various actions such as running commands, uploading and downloading files, and terminating processes. You can disable the ability to use the Live Terminal feature in Cortex XDR by configuring the Agent Settings Profile. The Agent Settings Profile defines the behavior and functionality of the Cortex XDR agent on the endpoint. You can create different profiles for different groups of endpoints and assign them accordingly. To disable the Live Terminal feature, you need to uncheck the Enable Live Terminal option in the Agent Settings Profile and save the changes. This will prevent the Cortex XDR agent from accepting any Live Terminal requests from the Cortex XDR management console. Reference:
Live Terminal: This document explains how to use the Live Terminal feature to investigate and respond to security events on Windows endpoints.
Agent Settings Profile: This document describes how to create and manage Agent Settings Profiles to define the behavior and functionality of the Cortex XDR agent on the endpoint.

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

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

Answer: A

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
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 # 19
.....

Exam Duration

- XDR-Analyst Practice Exam Questions ↕ New XDR-Analyst Test Guide □ XDR-Analyst Dumps Vce □ ➽ www.pass4test.com □ is best website to obtain ✔ XDR-Analyst □✔□ for free download □Latest Braindumps XDR-Analyst Ebook
- Why You Can Choose Palo Alto Networks XDR-Analyst Exam Questions? □ The page for free download of ☀ XDR-Analyst □☀□ on 【 www.pdfvce.com 】 will open immediately □XDR-Analyst Reliable Exam Prep
- Pass Guaranteed 2026 Palo Alto Networks XDR-Analyst Marvelous Study Tool □ The page for free download of ➠ XDR-Analyst □ on ➥ www.prep4away.com □ will open immediately □Valid XDR-Analyst Exam Pdf
- Palo Alto Networks XDR-Analyst exam pdf dumps □ Search for 《 XDR-Analyst 》 and download it for free on ▸ www.pdfvce.com ◂ website □Exam XDR-Analyst Tests
- Why You Can Choose Palo Alto Networks XDR-Analyst Exam Questions? □ Search for [XDR-Analyst] and obtain a free download on 《 www.prep4sures.top 》 □XDR-Analyst Valid Test Discount
- 2026 Study XDR-Analyst Tool | Reliable Palo Alto Networks XDR-Analyst Reliable Exam Book: Palo Alto Networks XDR Analyst ♥ Copy URL [www.pdfvce.com] open and search for ▹ XDR-Analyst ◃ to download for free □Relevant XDR-Analyst Questions
- XDR-Analyst Dumps Vce □ XDR-Analyst Exam Review □ XDR-Analyst Exam Study Guide □ Search for （ XDR-Analyst ） and download it for free on ➠ www.prepawaypdf.com □ website □XDR-Analyst Examcollection Vce
- zubairlflm053175.blogs100.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, express-page.com, nicolembwv621474.estate-blog.com, agnesapxi140889.wizzardsblog.com, philipnsab672533.dailyblogzz.com, janesfce641213.celticwiki.com, xanderrtii859965.law-wiki.com, janakydj365421.blogofchange.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