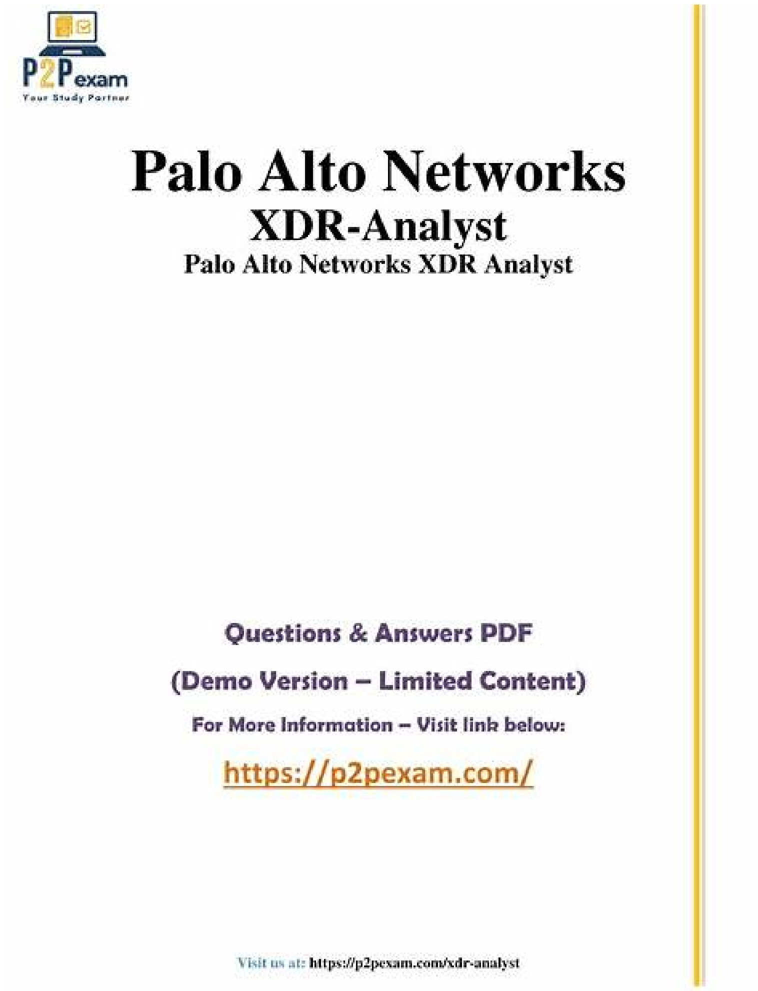
Pass Guaranteed 2026 Latest Palo Alto Networks XDR-Analyst: Reliable Palo Alto Networks XDR Analyst Exam Cost



Palo Alto Networks

XDR-Analyst

Palo Alto Networks XDR Analyst

Questions & Answers PDF

(Demo Version – Limited Content)

For More Information – Visit link below:

https://p2pexam.com/

Visit us at: https://p2pexam.com/xdr-analyst

Maybe you are unfamiliar with our XDR-Analyst latest material, but our XDR-Analyst real questions are applicable to this exam with high passing rate up to 98 percent and over. Choosing from a wide assortment of practice materials, rather than aiming solely to make a profit from our XDR-Analyst latest material, we are determined to offer help. Quick purchase process, free demos and various versions and high quality XDR-Analyst Real Questions are al features of our advantageous practice materials. With passing rate up to 98 to 100 percent, you will get through the XDR-Analyst practice exam with ease. So they can help you save time and cut down additional time to focus on the XDR-Analyst practice exam review only.

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	• 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 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	• 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.

Minimum XDR-Analyst Pass Score & Exam XDR-Analyst Cost

Palo Alto Networks XDR Analyst Sample Questions (Q55-Q60):

NEW QUESTION # 55
While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

- A. create an exception to prevent future false positives
- B. mark the incident as Resolved - False Positive
- C. create a BIOC rule excluding this behavior
- D. mark the incident as Unresolved

Answer: B

Explanation:
If all alerts contained in a Cortex XDR incident have exclusions, the Cortex XDR console will automatically mark the incident as Resolved - False Positive. This means that the incident was not a real threat, but a benign or legitimate activity that triggered an alert. By marking the incident as Resolved - False Positive, the Cortex XDR console removes the incident from the list of unresolved incidents and does not count it towards the incident statistics. This helps the analyst to focus on the true positive incidents that require further investigation and response1.
An exclusion is a rule that hides an alert from the Cortex XDR console, based on certain criteria, such as the alert source, type, severity, or description. An exclusion does not change the security policy or prevent the alert from firing, it only suppresses the alert from the console. An exclusion is useful when the analyst wants to reduce the noise of false positive alerts that are not relevant or important2.
An exception, on the other hand, is a rule that overrides the security policy and allows or blocks a process or file from running on an endpoint, based on certain attributes, such as the file hash, path, name, or signer. An exception is useful when the analyst wants to prevent false negative alerts that are caused by malicious or unwanted files or processes that are not detected by the security policy3.
A BIOC rule is a rule that creates an alert based on a custom XQL query that defines a specific behavior of interest or concern. A BIOC rule is useful when the analyst wants to detect and alert on anomalous or suspicious activities that are not covered by the default Cortex XDR rules4.
Reference:
Palo Alto Networks Cortex XDR Documentation, Resolve an Incident1
Palo Alto Networks Cortex XDR Documentation, Alert Exclusions2
Palo Alto Networks Cortex XDR Documentation, Exceptions3
Palo Alto Networks Cortex XDR Documentation, BIOC Rules4

NEW QUESTION # 56
Which of the following policy exceptions applies to the following description?
'An exception allowing specific PHP files'

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

Answer: B

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 # 57
What is the function of WildFire for Cortex XDR?

- A. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.
- B. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.
- C. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.
- D. WildFire accepts and analyses a sample to provide a verdict.

Answer: D

Explanation:
WildFire is a cloud-based service that accepts and analyses samples from various sources, including Cortex XDR, to provide a verdict of malware, benign, or grayware. WildFire also generates detailed analysis reports that show the behaviour and characteristics of the samples. Cortex XDR uses WildFire verdicts and reports to enhance its detection and prevention capabilities, as well as to provide more visibility and context into the threats. Reference:
WildFire Analysis Concepts
WildFire Overview

NEW QUESTION # 58
What is the Wildfire analysis file size limit for Windows PE files?

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

Answer: B

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 # 59
When creating a BIOC rule, which XQL query can be used?

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

Answer: C

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 # 60
......

If you're still studying hard to pass the Palo Alto Networks XDR-Analyst exam, Lead2Passed help you to achieve your dream. We provide you with the best Palo Alto Networks XDR-Analyst exam materials. It passed the test of practice, and with the best quality. It is better than Palo Alto Networks XDR-Analyst tutorials and any other related materials. It can help you to pass the Palo Alto Networks XDR-Analyst exam, and help you to become a strong IT expert.

Minimum XDR-Analyst Pass Score: https://www.lead2passed.com/Palo-Alto-Networks/XDR-Analyst-practice-exam-dumps.html

- Test XDR-Analyst Question □ Related XDR-Analyst Exams □ XDR-Analyst Latest Test Labs □ Simply search for { XDR-Analyst } for free download on ➡ www.easy4engine.com □□□ □PDF XDR-Analyst Download
- Reliable XDR-Analyst Real Test □ XDR-Analyst Latest Test Labs □ Online XDR-Analyst Tests □ Easily obtain free download of ➠ XDR-Analyst □ by searching on ➡ www.pdfvce.com □□□ □XDR-Analyst Free Exam Questions
- Free PDF Quiz 2026 Pass-Sure Palo Alto Networks XDR-Analyst: Reliable Palo Alto Networks XDR Analyst Exam Cost □ ▷ www.validtorrent.com ◁ is best website to obtain ✔ XDR-Analyst □✔□ for free download □Latest Braindumps XDR-Analyst Ppt
- Reliable XDR-Analyst Test Voucher □ XDR-Analyst Related Certifications □ Test XDR-Analyst Question □ Search for ⇒ XDR-Analyst ⇐ and obtain a free download on ▷ www.pdfvce.com ◁ □Test XDR-Analyst Question
- Authentic XDR-Analyst Learning Guide carries you pass-guaranteed Exam Questions - www.prep4away.com □ Search on ⇒ www.prep4away.com ⇐ for （ XDR-Analyst ） to obtain exam materials for free download □XDR-Analyst Sample Questions
- XDR-Analyst Actual Questions Update in a High Speed - Pdfvce □ Easily obtain ⇒ XDR-Analyst ⇐ for free download through □ www.pdfvce.com □ □XDR-Analyst Latest Test Questions
- Valid Reliable XDR-Analyst Exam Cost | 100% Free Minimum XDR-Analyst Pass Score □ The page for free download of ☀ XDR-Analyst □☀□ on ⇒ www.prepawayete.com ⇐ will open immediately □XDR-Analyst Reliable Test Duration
- Get the Real Palo Alto Networks XDR-Analyst Exam Dumps In Different Formats □ Search on 「 www.pdfvce.com 」 for ▶ XDR-Analyst ◀ to obtain exam materials for free download □XDR-Analyst Sample Questions
- Latest Braindumps XDR-Analyst Ppt □ XDR-Analyst Sample Questions □ XDR-Analyst Latest Exam Answers □ Search for □ XDR-Analyst □ and download it for free on ➤ www.practicevce.com □ website □XDR-Analyst Related Certifications
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ilmannafiya.org, lms.rilosmals.com, bbs.t-firefly.com, writeablog.net, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes