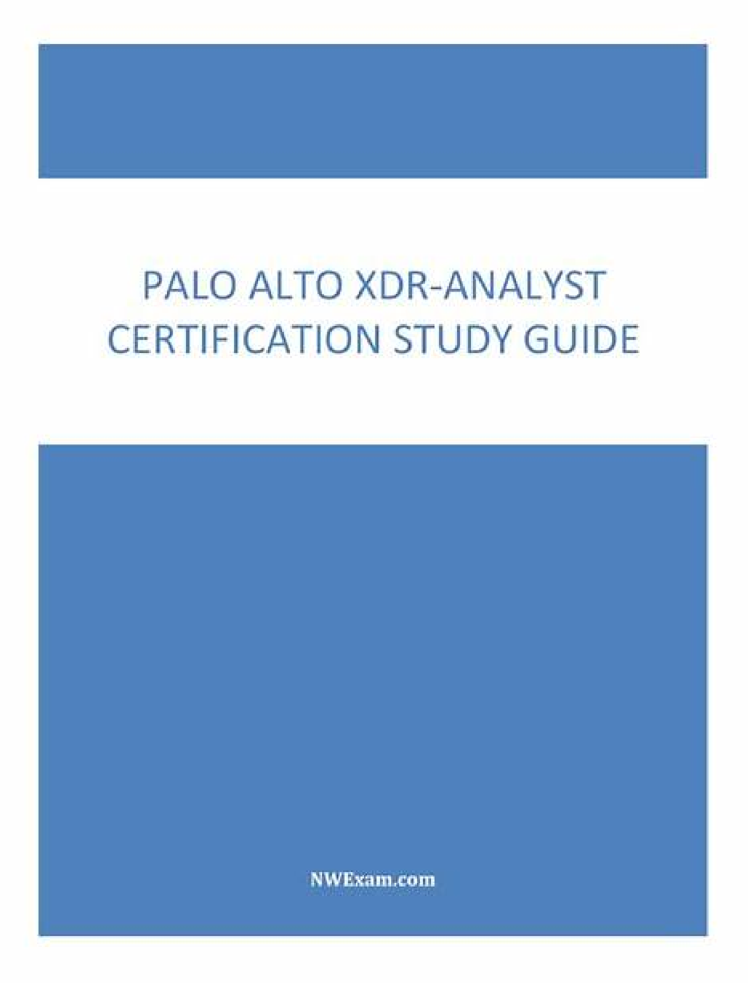
Windows-based Palo Alto Networks XDR-Analyst Practice Exam Software



PALO ALTO XDR-ANALYST
CERTIFICATION STUDY GUIDE

NWExam.com

Due to continuous efforts of our experts, we have exactly targeted the content of the XDR-Analyst exam. You will pass the XDR-Analyst exam after 20 to 30 hours' learning with our XDR-Analyst study material. If you fail to pass the exam, we will give you a refund. Many users have witnessed the effectiveness of our XDR-Analyst Guide braindumps you surely will become one of them. Try it right now! And we will let you down.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	- 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 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	- 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 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.

XDR-Analyst Reliable Test Cram - XDR-Analyst Exam Tutorials

Our XDR-Analyst research materials are widely known throughout the education market. Almost all the candidates who are ready for the qualifying examination know our products. Even when they find that their classmates or colleagues are preparing a XDR-Analyst exam, they will introduce our study materials to you. So, our learning materials help users to be assured of the XDR-Analyst Exam. Currently, my company has introduced a variety of learning materials, covering almost all the official certification of qualification exams, and each XDR-Analyst learning materials in our online store before the listing, are subject to stringent quality checks within the company.

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

NEW QUESTION # 15
Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

- A. Data Ingestion Dashboard
- B. Security Admin Dashboard
- C. Security Manager Dashboard
- D. Incident Management Dashboard

Answer: D

Explanation:
The Incident Management Dashboard provides a high-level overview of the incident response process, including the Mean Time to Resolution (MTTR) metric. This metric measures the average time it takes to resolve an incident from the moment it is created to the moment it is closed. The dashboard also shows the number of incidents by status, severity, and assigned analyst, as well as the top alerts by category, source, and destination. The Incident Management Dashboard is designed for executives and managers who want to monitor the performance and efficiency of their security teams. Reference: [PCDRA Study Guide], page 18.

NEW QUESTION # 16
When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. It is blank
- B. Pending
- C. Unassigned
- D. New

Answer: C

Explanation:
The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
B . It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group12.
D . New: This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status"

field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.
Reference:
Cortex XDR Pro Admin Guide: Manage Incidents
Cortex XDR Pro Admin Guide: Assign Incidents
Cortex XDR Pro Admin Guide: Update Incident Status

NEW QUESTION # 17
Which of the following represents the correct relation of alerts to incidents?

- A. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- B. Alerts that occur within a three-hour time frame are grouped together into one Incident.
- C. Every alert creates a new Incident.
- D. Only alerts with the same host are grouped together into one Incident in a given time frame.

Answer: A

Explanation:
The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details1.
Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.
Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2 Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

NEW QUESTION # 18
Can you disable the ability to use the Live Terminal feature in Cortex XDR?

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

Answer: B

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 # 19

Under which conditions is Local Analysis evoked to evaluate a file before the file is allowed to run?

- A. The endpoint is disconnected or the verdict from WildFire is of a type benign.
- B. The endpoint is disconnected or the verdict from WildFire is of a type malware.
- C. The endpoint is disconnected or the verdict from WildFire is of a type grayware.
- D. The endpoint is disconnected or the verdict from WildFire is of a type unknown.

Answer: D

Explanation:
Local Analysis is a feature of Cortex XDR that allows the agent to evaluate files locally on the endpoint, without sending them to WildFire for analysis. Local Analysis is evoked when the following conditions are met:
The endpoint is disconnected from the internet or the Cortex XDR management console, and therefore cannot communicate with WildFire.
The verdict from WildFire is of a type unknown, meaning that WildFire has not yet analyzed the file or has not reached a conclusive verdict.
Local Analysis uses machine learning models to assess the behavior and characteristics of the file and assign it a verdict of either benign, malware, or grayware. If the verdict is malware or grayware, the agent will block the file from running and report it to the Cortex XDR management console. If the verdict is benign, the agent will allow the file to run and report it to the Cortex XDR management console. Reference:
Local Analysis
WildFire File Verdicts

NEW QUESTION # 20

......

The pass rate is 98%, and we also pass guarantee if you buy XDR-Analyst study materials of us. We have received many good feedbacks of the XDR-Analyst exam dups. You also enjoy free update for one year after your payment, and if you have any questions about the XDR-Analyst Exam Dumps, just ask our online service stuff, they will give a reply immediately, or you can send email to us, we will answer you as quickly as we can. Therefore, just contact us if you have the confusions about the XDR-Analyst study materials.

XDR-Analyst Reliable Test Cram: https://www.troytecdumps.com/XDR-Analyst-troytec-exam-dumps.html

- Reliable XDR-Analyst Dumps Ppt □ XDR-Analyst Reliable Study Notes □ Reliable XDR-Analyst Dumps Ppt □ Immediately open ➡ www.practicevce.com □□□ and search for □ XDR-Analyst □ to obtain a free download □Reliable XDR-Analyst Dumps Ppt
- XDR-Analyst Sample Questions □ XDR-Analyst Braindump Pdf □ XDR-Analyst Valid Exam Tips □ □ www.pdfvce.com □ is best website to obtain 《 XDR-Analyst 》 for free download □100% XDR-Analyst Exam Coverage
- Exam XDR-Analyst Topic □ Latest XDR-Analyst Examprep □ XDR-Analyst Valid Exam Tips □ □ www.examcollectionpass.com □ is best website to obtain 「 XDR-Analyst 」 for free download □XDR-Analyst Latest Test Vce
- Hot XDR-Analyst Latest Exam Free PDF | Pass-Sure XDR-Analyst Reliable Test Cram: Palo Alto Networks XDR Analyst □ Simply search for □ XDR-Analyst □ for free download on ➽ www.pdfvce.com □ □Latest XDR-Analyst Examprep
- 100% XDR-Analyst Exam Coverage □ 100% XDR-Analyst Exam Coverage □ XDR-Analyst Free Updates □ Download ☀ XDR-Analyst □☀□ for free by simply entering 【 www.troytecdumps.com 】 website □XDR-Analyst Practice Engine
- Palo Alto Networks XDR-Analyst Exam Questions - Easy Way To Prepare [2026] □ Enter ➤ www.pdfvce.com □ and search for ➠ XDR-Analyst □ to download for free □XDR-Analyst Reliable Study Notes
- XDR-Analyst Braindump Pdf □ Exam XDR-Analyst Topic □ Simulated XDR-Analyst Test □ Copy URL ▹

www.prepawaypdf.com ◁ open and search for 「 XDR-Analyst 」 to download for free □XDR-Analyst Sample Questions

- Hot XDR-Analyst Latest Exam Free PDF | Pass-Sure XDR-Analyst Reliable Test Cram: Palo Alto Networks XDR Analyst □ Search for ➽ XDR-Analyst □ on □ www.pdfvce.com □ immediately to obtain a free download □XDR-Analyst Reliable Test Prep
- Ace Your XDR-Analyst Exam with Palo Alto Networks's Exam Questions and Achieve Success □ Search for ▶ XDR-Analyst ◀ and easily obtain a free download on 【 www.prep4away.com 】 ✏Updated XDR-Analyst Dumps
- 2026 Palo Alto Networks XDR-Analyst Accurate Latest Exam □ Simply search for ➤ XDR-Analyst □ for free download on □ www.pdfvce.com □ □XDR-Analyst Reliable Study Notes
- Valid Test XDR-Analyst Vce Free □ XDR-Analyst Latest Test Vce ☣ XDR-Analyst Sample Questions □ Search for ➠ XDR-Analyst □ and download exam materials for free through □ www.examcollectionpass.com □ □New XDR-Analyst Exam Sample
- www.stes.tyc.edu.tw, telegra.ph, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, 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