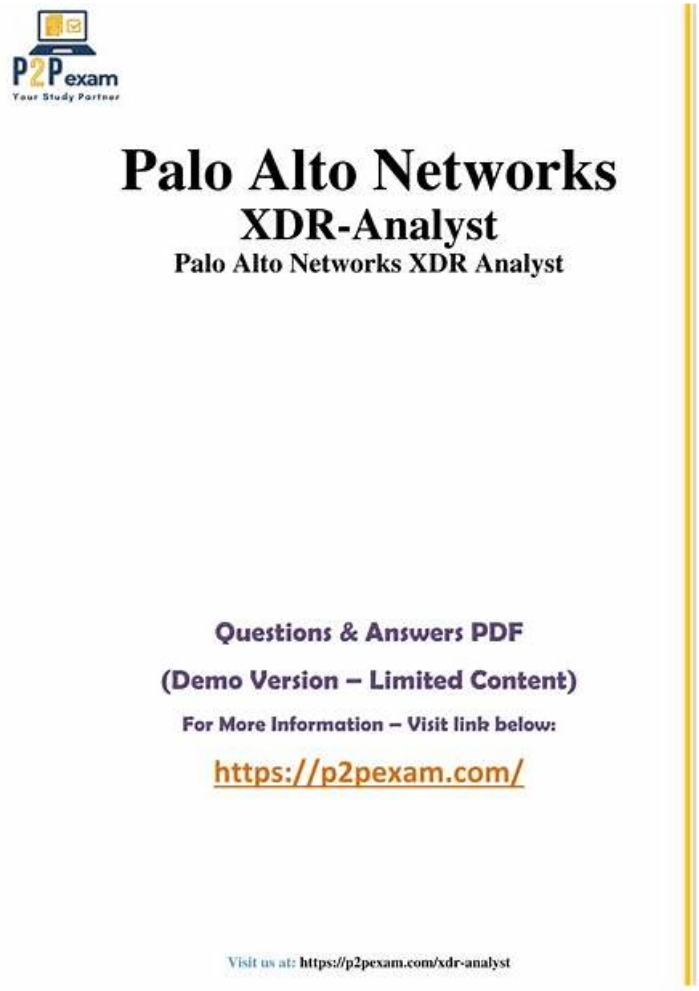
Free PDF Quiz Palo Alto Networks - XDR-Analyst - Trustable Reliable Palo Alto Networks XDR Analyst Exam Blueprint



The XDR-Analyst study quiz is made from various experts for examination situation in recent years in the field of systematic analysis of finishing, meet the demand of the students as much as possible, at the same time have a professional staff to check and review XDR-Analyst practice materials, made the learning of the students enjoy the information of high quality. Due to the variety of examinations, so that students can find the information on XDR-Analyst guide engine they need quickly.

According to the survey from our company, the experts and professors from our company have designed and compiled the best XDR-Analyst cram guide in the global market. We can assure to all people that our XDR-Analyst study materials will have a higher quality and it can help all people to remain an optimistic mind when they are preparing for the XDR-Analyst Exam. On the contrary, people who want to pass the exam will persist in studying all the time. We deeply believe that the latest XDR-Analyst study questions from our company will is most suitable and helpful for all people.

>> Reliable XDR-Analyst Exam Blueprint <<

Latest XDR-Analyst Dumps - XDR-Analyst Test Answers

If you are new to our XDR-Analyst exam questions, you may doubt about them a lot. And that is normal. Many of our loyal customers first visited our website, or even they have bought and studied with our XDR-Analyst practice engine, they would worried a lot. But when they finally passed the exam with our XDR-Analyst simulating exam, they knew that it is valid and helpful. And we also have free demos on our website, then you will know the quality of our XDR-Analyst training quiz.

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	• Endpoint Security Management:
Topic 3	• 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.
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.

Palo Alto Networks XDR Analyst Sample Questions (Q59-Q64):

NEW QUESTION # 59
What should you do to automatically convert leads into alerts after investigating a lead?

- A. Build a search query using Query Builder or XQL using a list of IOCs.
- B. Lead threats can't be prevented in the future because they already exist in the environment.
- C. Create BIOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.
- D. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

Answer: D

Explanation:
To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. Reference:
PCDRA Study Guide, page 25
Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2
Cortex XDR Documentation, section "Create IOC Rules"

NEW QUESTION # 60
Which of the following represents the correct relation of alerts to incidents?

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

Answer: C

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 # 61
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 a global exception.
- B. Create an individual alert exclusion.
- C. Create an endpoint-specific exception.
- D. Create a global inclusion.

Answer: A

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 # 62
Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

- A. exception profiles that apply to specific endpoints
- B. global exception profiles that apply to all endpoints
- C. role-based profiles that apply to specific endpoints
- D. agent exception profiles that apply to specific endpoints

Answer: B,D

Explanation:
Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. Reference:
Exception Security Profiles
Create an Agent Exception Profile
Create a Global Exception Profile

NEW QUESTION # 63
What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

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

Answer: A

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 # 64
.....

Passing the XDR-Analyst exam requires many abilities of you: personal ability, efficient practice materials, as well as a small touch of luck. So your personal effort is brilliant but insufficient to pass exam, and our XDR-Analyst exam materials can facilitate the process smoothly and successfully. Our XDR-Analyst Study Dumps are suitable for you whichever level you are in right now. Whether you are in entry-level position or experienced exam candidates who have tried the exam before, this is the perfect chance to give a shot.

Latest XDR-Analyst Dumps: https://www.exams-boost.com/XDR-Analyst-valid-materials.html

- Exam XDR-Analyst Details □ XDR-Analyst Free Test Questions □ XDR-Analyst Pass4sure Study Materials □ Immediately open □ www.prepawayexam.com □ and search for ▸ XDR-Analyst ◂ to obtain a free download □XDR-Analyst Free Test Questions
- Using the XDR-Analyst Exam Questions to get pass ↘ Download ▸ XDR-Analyst ◂ for free by simply entering ➽ www.pdfvce.com □ website □XDR-Analyst Valid Dumps Pdf
- Quiz XDR-Analyst - Palo Alto Networks XDR Analyst Perfect Reliable Exam Blueprint □ Enter ➥ www.examdiscuss.com □ and search for ➽ XDR-Analyst □ to download for free □XDR-Analyst Latest Exam Practice
- Pass Guaranteed Valid XDR-Analyst - Reliable Palo Alto Networks XDR Analyst Exam Blueprint □ Immediately open { www.pdfvce.com } and search for ▹ XDR-Analyst ◃ to obtain a free download □XDR-Analyst Quiz
- Online XDR-Analyst Training □ New XDR-Analyst Exam Simulator □ XDR-Analyst Quiz □ Search for □ XDR-Analyst □ and easily obtain a free download on 《 www.prep4away.com 》 □XDR-Analyst Related Certifications
- Palo Alto Networks XDR Analyst Certification Materials Can Alleviated Your Pressure from XDR-Analyst certification - Pdfvce □ ➡ www.pdfvce.com □□□ is best website to obtain （ XDR-Analyst ） for free download □New XDR-Analyst Test Prep
- Palo Alto Networks XDR Analyst Certification Materials Can Alleviated Your Pressure from XDR-Analyst certification - www.prepawayete.com □ Open website ⇛ www.prepawayete.com ⇚ and search for ➠ XDR-Analyst □ for free download □New XDR-Analyst Test Prep
- Pass Guaranteed Palo Alto Networks - High Pass-Rate Reliable XDR-Analyst Exam Blueprint □ Simply search for 《

XDR-Analyst》 for free download on ➥ www.pdfvce.com □ □Certification XDR-Analyst Exam Dumps

- Pass Guaranteed Palo Alto Networks - High Pass-Rate Reliable XDR-Analyst Exam Blueprint □ Download ✔ XDR-Analyst □✔□ for free by simply searching on □ www.prepawayete.com □ □XDR-Analyst Valid Test Online
- Pass Guaranteed Palo Alto Networks - High Pass-Rate Reliable XDR-Analyst Exam Blueprint □ Open website ➥ www.pdfvce.com □ and search for ➡ XDR-Analyst □□□ for free download □New XDR-Analyst Test Prep
- Certification XDR-Analyst Exam Dumps □ XDR-Analyst Exam Cram Pdf □ XDR-Analyst Exam Cram Pdf □ Open ➠ www.prepawaypdf.com □ and search for 「 XDR-Analyst 」 to download exam materials for free □XDR-Analyst Valid Braindumps Free
- www.stes.tyc.edu.tw, jobs.electronicsweekly.com, www.stes.tyc.edu.tw, www.intensedebate.com, hhi.instructure.com, www.divephotoguide.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pinoyseo.ph, experiment.com, Disposable vapes