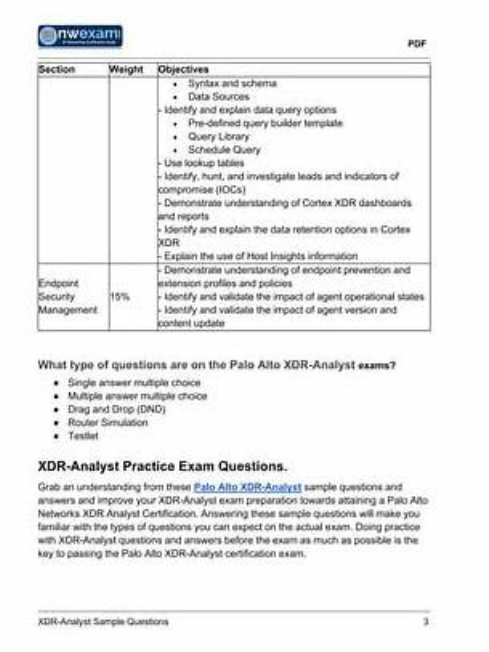
Newest Study XDR-Analyst Dumps, XDR-Analyst Practice Test Pdf



nwexam

PDF

Section	Weight	Objectives
		• Syntax and schema • Data Sources - Identify and explain data query options • Pre-defined query builder template • Query Library • Schedule Query - Use lookup tables - Identify, hunt, and investigate leads and indicators of compromise (IOCs) - Demonstrate understanding of Cortex XDR dashboards and reports - Identify and explain the data retention options in Cortex XDR - Explain the use of Host Insights information
Endpoint Security Management	15%	- Demonstrate understanding of endpoint prevention and extension profiles and policies - Identify and validate the impact of agent operational states - Identify and validate the impact of agent version and content update

What type of questions are on the Palo Alto XDR-Analyst exams?

- Single answer multiple choice
- Multiple answer multiple choice
- Drag and Drop (DND)
- Router Simulation
- Testlet

XDR-Analyst Practice Exam Questions.

Grab an understanding from these Palo Alto XDR-Analyst sample questions and answers and improve your XDR-Analyst exam preparation towards attaining a Palo Alto Networks XDR Analyst Certification. Answering these sample questions will make you familiar with the types of questions you can expect on the actual exam. Doing practice with XDR-Analyst questions and answers before the exam as much as possible is the key to passing the Palo Alto XDR-Analyst certification exam.

XDR-Analyst Sample Questions 3

BTW, DOWNLOAD part of Exams4sures XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=11iU0uyrySa73cc2OM-XieNW72zlqfJkS

Palo Alto Networks XDR Analyst (XDR-Analyst) PDF dumps are the third and most convenient format of the Palo Alto Networks XDR-Analyst PDF questions prep material. This format is perfect for busy test takers who prefer to study for the Palo Alto Networks XDR Analyst (XDR-Analyst) exam on the go. Questions bank in the Exams4sures Palo Alto Networks XDR-Analyst Pdf Dumps is accessible via all smart devices. We also update Palo Alto Networks XDR Analyst (XDR-Analyst) PDF questions regularly to ensure they match with the new content of the XDR-Analyst exam.

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	• 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	• 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 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.

>> Study XDR-Analyst Dumps <<

Advantages Of Web-Based Palo Alto Networks XDR-Analyst Practice Tests

By concluding quintessential points into Palo Alto Networks XDR Analyst practice materials, you can pass the exam with the least time while huge progress. Our experts are responsible to make in-depth research on the exams who contribute to growth of our XDR-Analyst practice materials. Their highly accurate exam point can help you detect flaws on the review process and trigger your enthusiasm about the exam. What is more, XDR-Analyst practice materials can fuel your speed and the professional backup can relieve you of stress of the challenge.

Palo Alto Networks XDR Analyst Sample Questions (Q90-Q95):

NEW QUESTION # 90
When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

- A. The prevention archive from the alert.
- B. The unique agent id.
- C. The distribution id of the agent.
- D. The agent technical support file.
- E. A list of all the current exceptions applied to the agent.

Answer: A,D

Explanation:
When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:
The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.
The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.
The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:
The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.
A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.
The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.
Reference:
Generate and Download the Agent Technical Support File
Generate and Download the Prevention Archive
Cortex XDR Agent Administrator Guide: Agent Distribution ID

Cortex XDR Agent Administrator Guide: Exception Security Profiles
[Cortex XDR Agent Administrator Guide: Unique Agent ID]

NEW QUESTION # 91
Which of the following policy exceptions applies to the following description?
'An exception allowing specific PHP files'

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

Answer: C

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 # 92
In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

- A. Salesforce
- B. Service Now
- C. Jira
- D. Slack

Answer: D

Explanation:
Cortex XDR allows you to schedule reports and forward them to Slack, a cloud-based collaboration platform. You can configure the Slack channel, frequency, and recipients of the scheduled reports. You can also view the report history and status in the Cortex XDR management console. Reference:
Scheduled Queries: This document explains how to create, edit, and manage scheduled queries and reports in Cortex XDR.
Forward Scheduled Reports to Slack: This document provides the steps to configure Slack integration and forward scheduled reports to a Slack channel.

NEW QUESTION # 93
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically close the connections involved in malicious traffic.
- B. Automatically terminate the threads involved in malicious activity.
- C. Automatically kill the processes involved in malicious activity.
- D. Automatically block the IP addresses involved in malicious traffic.

Answer: C,D

NEW QUESTION # 94
To stop a network-based attack, any interference with a portion of the attack pattern is enough to prevent it from succeeding. Which statement is correct regarding the Cortex XDR Analytics module?

- A. It does not interfere with any portion of the pattern on the endpoint.
- B. It does not need to interfere with the any portion of the pattern to prevent the attack.
- C. It interferes with the pattern as soon as it is observed by the firewall.
- D. It interferes with the pattern as soon as it is observed on the endpoint.

Answer: D

Explanation:
The correct statement regarding the Cortex XDR Analytics module is D, it interferes with the pattern as soon as it is observed on the endpoint. The Cortex XDR Analytics module is a feature of Cortex XDR that uses machine learning and behavioral analytics to detect and prevent network-based attacks on endpoints. The Cortex XDR Analytics module analyzes the network traffic and activity on the endpoint, and compares it with the attack patterns defined by Palo Alto Networks threat research team. The Cortex XDR Analytics module interferes with the attack pattern as soon as it is observed on the endpoint, by blocking the malicious network connection, process, or file. This way, the Cortex XDR Analytics module can stop the attack before it causes any damage or compromise.
The other statements are incorrect for the following reasons:
A is incorrect because the Cortex XDR Analytics module does interfere with the attack pattern on the endpoint, by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on the firewall or any other network device to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.
B is incorrect because the Cortex XDR Analytics module does not interfere with the attack pattern as soon as it is observed by the firewall. The Cortex XDR Analytics module does not depend on the firewall or any other network device to detect or prevent the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the analysis and interference. The firewall may not be able to observe or block the attack pattern if it is encrypted, obfuscated, or bypassed by the attacker.
C is incorrect because the Cortex XDR Analytics module does need to interfere with the attack pattern to prevent the attack. The Cortex XDR Analytics module does not only detect the attack pattern, but also prevents it from succeeding by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on any other response mechanism or human intervention to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.
Reference:
Cortex XDR Analytics Module
Cortex XDR Analytics Module Detection and Prevention

NEW QUESTION # 95
.....

Passing the exam rests squarely on the knowledge of exam questions and exam skills. Our XDR-Analyst training quiz has bountiful content that can fulfill your aims at the same time. We know high efficient XDR-Analyst practice materials play crucial roles in your review. Our experts also collect with the newest contents and have been researching where the exam trend is heading and what it really want to examine you. By analyzing the syllabus and new trend, our XDR-Analyst Practice Engine is totally in line with this exam for your reference. So grapple with this chance, our XDR-Analyst practice materials will not let you down.

□ XDR-Analyst □ to download for free □XDR-Analyst Exam Dumps Provider

- XDR-Analyst Exam Sample □ Valid XDR-Analyst Exam Voucher □ XDR-Analyst Valid Test Registration □ Copy URL □ www.dumpsmaterials.com □ open and search for 《 XDR-Analyst 》 to download for free □XDR-Analyst Valid Test Guide
- Quiz 2026 Useful XDR-Analyst: Study Palo Alto Networks XDR Analyst Dumps □ Search for ➥ XDR-Analyst □ and easily obtain a free download on ▷ www.pdfvce.com ◁ □Exam Questions XDR-Analyst Vce
- How Palo Alto Networks XDR-Analyst PDF Dumps is essential on your XDR-Analyst Exam Questions Certain Success □ □ Copy URL ☀ www.exam4labs.com □☀□ open and search for 【 XDR-Analyst 】 to download for free □XDR-Analyst Valid Test Guide
- fortunetelleroracle.com, estar.jp, hanson.net, www.bandlab.com, estar.jp, telegra.ph, ummalife.com, kaeuchi.jp, hashnode.com, scalar.usc.edu, Disposable vapes

P.S. Free & New XDR-Analyst dumps are available on Google Drive shared by Exams4sures: https://drive.google.com/open?id=11iU0uyrySa73cc2OM-XieNW72zlqfJkS