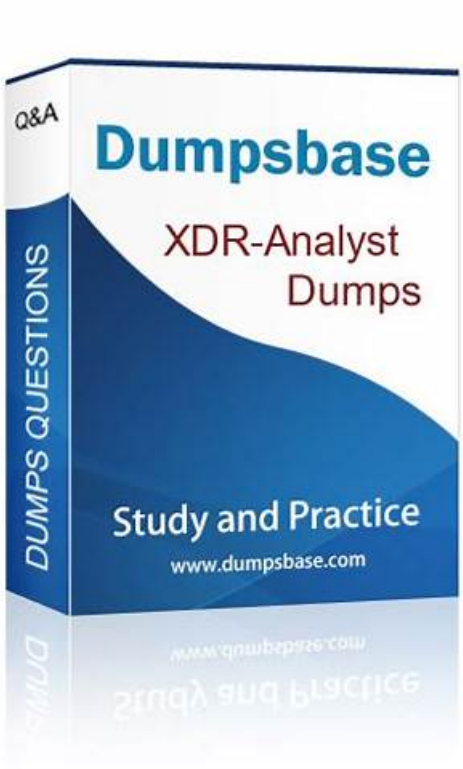
Marvelous XDR-Analyst Valid Test Topics & Leading Offer in Qualification Exams & Trusted Free XDR-Analyst Updates



P.S. Free 2026 Palo Alto Networks XDR-Analyst dumps are available on Google Drive shared by VerifiedDumps: https://drive.google.com/open?id=1dAGdtkrEpRXyHx795XF73KwsOeif51a1

Palo Alto Networks certification XDR-Analyst exams has become more and more popular in the fiercely competitive IT industry. Although more and more people sign up to attend this examination of, the official did not reduce its difficulty and it is still difficult to pass the exam. After all, this is an authoritative test to inspect the computer professional knowledge and information technology ability. In order to pass the Palo Alto Networks Certification XDR-Analyst Exam, generally, many people need to spend a lot of time and effort to review.

Do you want to pass your exam by using the latest time? If you do, you can choose the XDR-Analyst study guide of us. We can help you pass the exam just one time. With experienced experts to compile and verify the XDR-Analyst exam dumps, the quality and accuracy can be guaranteed. Therefore, you just need to spend 48 to 72 hours on training, you can pass the exam. In addition, we offer you free demo to have a try before buying XDR-Analyst Study Guide, so that you can know what the complete version is like. Our online and offline chat service stuff will give you reply of all your confusions about the XDR-Analyst exam dumps.

>> XDR-Analyst Valid Test Topics <<

Free PDF XDR-Analyst Valid Test Topics & Efficient Free XDR-Analyst Updates: Palo Alto Networks XDR Analyst

Immediately after you have made a purchase for our XDR-Analyst practice dumps, you can download our XDR-Analyst study materials to make preparations. It is universally acknowledged that time is a key factor in terms of the success. The more time you spend in the preparation for XDR-Analyst Training Materials, the higher possibility you will pass the exam. And with our XDR-Analyst study torrent, you can get preparations and get success as early as possible.

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	• 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	• 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.

Palo Alto Networks XDR Analyst Sample Questions (Q26-Q31):

NEW QUESTION # 26
Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques.

- A. Exfiltration, Command and Control, Collection
- B. Exfiltration, Command and Control, Privilege Escalation
- C. Exfiltration, Command and Control, Lateral Movement
- D. Exfiltration, Command and Control, Impact

Answer: C

Explanation:
Cortex XDR Analytics is a feature of Cortex XDR that leverages machine learning and behavioral analytics to detect and alert on malicious activity across the network and endpoint layers. Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques: Exfiltration, Command and Control, Lateral Movement, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection. However, among the options given in the question, the correct answer is D, Exfiltration, Command and Control, Lateral Movement. These are three of the most critical techniques that indicate an advanced and persistent threat (APT) in the environment. Exfiltration refers to the technique of transferring data or information from the compromised system or network to an external location controlled by the adversary. Command and Control refers to the technique of communicating with the compromised system or network to provide instructions, receive data, or update malware. Lateral Movement refers to the technique of moving from one system or network to another within the same environment, usually to gain access to more resources or data. Cortex XDR Analytics can alert on these techniques by analyzing various data sources, such as network traffic, firewall logs, endpoint events, and threat intelligence, and applying behavioral models, anomaly detection, and correlation rules. Cortex XDR Analytics can also map the alerts to the corresponding MITRE ATT&CKTM techniques and provide additional context and visibility into the attack chain1234 Reference:
Cortex XDR Analytics
MITRE ATT&CKTM
Cortex XDR Analytics MITRE ATT&CKTM Techniques
Cortex XDR Analytics Alert Categories

NEW QUESTION # 27
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

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

Answer: C,D

NEW QUESTION # 28
What is the difference between presets and datasets in XQL?

- A. A dataset is a database; presets is a field.
- B. A dataset is a Cortex data lake data source only; presets are built-in data source.
- C. A dataset is a built-in or third-party source; presets group XDR data fields.
- D. A dataset is a third-party data source; presets are built-in data source.

Answer: C

Explanation:
The difference between presets and datasets in XQL is that a dataset is a built-in or third-party data source, while a preset is a group of XDR data fields. A dataset is a collection of data that you can query and analyze using XQL. A dataset can be a Cortex data lake data source, such as endpoints, alerts, incidents, or network flows, or a third-party data source, such as AWS CloudTrail, Azure Activity Logs, or Google Cloud Audit Logs. A preset is a predefined set of XDR data fields that are relevant for a specific use case, such as process execution, file operations, or network activity. A preset can help you simplify and standardize your XQL queries by selecting the most important fields for your analysis. You can use presets with any Cortex data lake data source, but not with third-party data sources. Reference:
Datasets and Presets
XQL Language Reference

NEW QUESTION # 29
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

- A. NetBIOS over TCP
- B. TCP, over port 80
- C. WebSocket
- D. UDP and a random port

Answer: C

Explanation:
Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. Reference:
Initiate a Live Terminal Session
WebSocket

NEW QUESTION # 30
When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

- A. Delete the selected Incidents.
- B. Investigate several Incidents at once.
- C. Change the status of multiple incidents.
- D. Assign incidents to an analyst in bulk.

Answer: C,D

Explanation:
When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved,

or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 Reference:
Assign Incidents to an Analyst in Bulk
Change the Status of Multiple Incidents

NEW QUESTION # 31
.....

Wondering where you can find the perfect materials for the exam? Don't leave your fate depending on thick books about the XDR-Analyst exam. Our authoritative XDR-Analyst study materials are licensed products. Whether newbie or experienced exam candidates you will be eager to have our XDR-Analyst Exam Questions. And they all made huge advancement after using them. Not only that you will get the certification, but also you will have more chances to get higher incomes and better career.