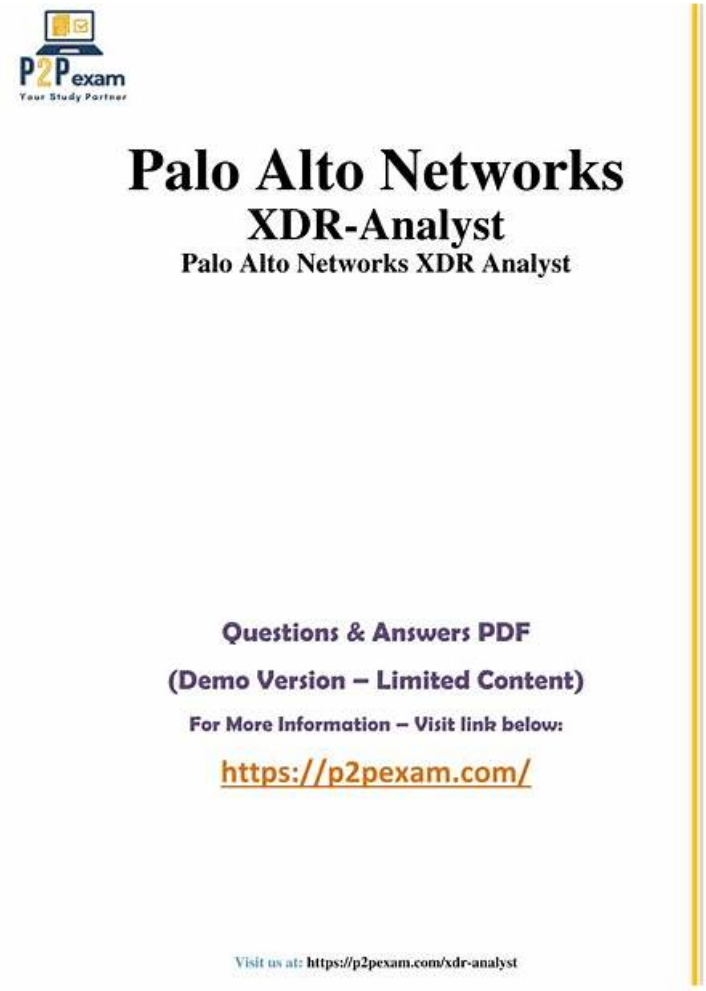
Three Palo Alto Networks XDR-Analyst Exam Practice Questions Formats



The students can give unlimited to track the performance of their last given tests in order to see their mistakes and try to avoid them while giving the final test. Customers of Easy4Engine will receive updates till 1 year after their purchase. Anyone can try a free demo of the Palo Alto Networks XDR Analyst (XDR-Analyst) practice material before making purchase. There is a 24/7 available support system that assists users whenever they are stuck in any problem or issues. This product is a complete package and a blessing for those who want to pass the Palo Alto Networks XDR-Analyst test in a single try.

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.

>> Reliable XDR-Analyst Test Cost <<

Palo Alto Networks XDR-Analyst Exam Lab Questions, Frenquent XDR-Analyst Update

If you are still worried about your exam, our exam dumps may be your good choice. Our Palo Alto Networks XDR-Analyst training dumps cover many real test materials so that if you master our dumps questions and answers you can clear exams successfully. Don't worry over trifles. If you purchase our Palo Alto Networks XDR-Analyst training dumps you can spend your time on more significative work.

Palo Alto Networks XDR Analyst Sample Questions (Q36-Q41):

NEW QUESTION # 36
When using the "File Search and Destroy" feature, which of the following search hash type is supported?

- A. AES256 hash of the file
- B. MD5 hash of the file
- C. SHA1 hash of the file
- D. SHA256 hash of the file

Answer: D

Explanation:
The File Search and Destroy feature is a capability of Cortex XDR that allows you to search for and delete malicious or unwanted files across your endpoints. You can use this feature to quickly respond to incidents, remediate threats, and enforce compliance policies. To use the File Search and Destroy feature, you need to specify the file name and the file hash of the file you want to search for and delete. The file hash is a unique identifier of the file that is generated by a cryptographic hash function. The file hash ensures that you are targeting the exact file you want, and not a file with a similar name or a different version. The File Search and Destroy feature supports the SHA256 hash type, which is a secure hash algorithm that produces a 256-bit (32-byte) hash value. The SHA256 hash type is widely used for file integrity verification and digital signatures. The File Search and Destroy feature does not support other hash types, such as AES256, MD5, or SHA1, which are either encryption algorithms or less secure hash algorithms. Therefore, the correct answer is A, SHA256 hash of the file1234 Reference:
File Search and Destroy
What is a File Hash?
SHA-2 - Wikipedia
When using the "File Search and Destroy" feature, which of the following search hash type is supported?

NEW QUESTION # 37
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

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

Answer: A,B

NEW QUESTION # 38
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

- A. TCP, over port 80

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

Answer: D

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 # 39
Which minimum Cortex XDR agent version is required for Kubernetes Cluster?

- A. Cortex XDR 6.1
- B. Cortex XDR 5.0
- C. Cortex XDR 7.5
- D. Cortex XDR 7.4

Answer: C

Explanation:
The minimum Cortex XDR agent version required for Kubernetes Cluster is Cortex XDR 7.5. This version introduces the Cortex XDR agent for Kubernetes hosts, which provides protection and visibility for Linux hosts that run on Kubernetes clusters. The Cortex XDR agent for Kubernetes hosts supports the following features:
Anti-malware protection
Behavioral threat protection
Exploit protection
File integrity monitoring
Network security
Audit and remediation
Live terminal
To install the Cortex XDR agent for Kubernetes hosts, you need to deploy the Cortex XDR agent as a DaemonSet on your Kubernetes cluster. You also need to configure the agent settings profile and the agent installer in the Cortex XDR management console. Reference:
Cortex XDR Agent Release Notes: This document provides the release notes for Cortex XDR agent versions, including the new features, enhancements, and resolved issues.
Install the Cortex XDR Agent for Kubernetes Hosts: This document explains how to install and configure the Cortex XDR agent for Kubernetes hosts using the Cortex XDR management console and the Kubernetes command-line tool.

NEW QUESTION # 40
Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

- A. Quarantine
- B. Search & destroy
- C. Flag for removal
- D. Isolation

Answer: A

Explanation:
The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or

suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. Reference:
Quarantine Files
Manage Quarantined Files

NEW QUESTION # 41
.....

Obtaining a certificate is not only an affirmation of your ability, but also can improve your competitive force in the job market. XDR-Analyst exam materials will help you pass the exam and get the certificate successfully. You just need to spend some money and you can get the certificate. In addition, we have a professional team to collect the latest information about the XDR-Analyst Exam Materials, we can ensure you that what you get is the latest version we have. We offer you free update for 365 days after purchasing, and the update version for XDR-Analyst exam dumps will be sent to your email automatically.