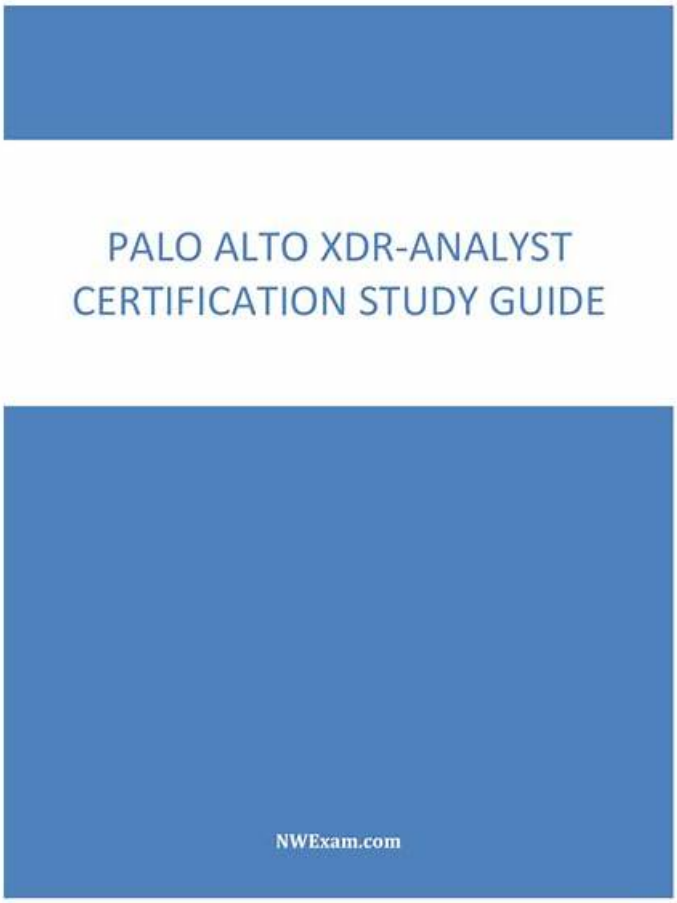
XDR-Analyst Latest Test Dumps - Exam XDR-Analyst Guide Materials



With over a decade's business experience, our XDR-Analyst test torrent attached great importance to customers' purchasing rights all along. There is no need to worry about virus on buying electronic products. For we make endless efforts to assess and evaluate our XDR-Analyst exam prep' reliability for a long time and put forward a guaranteed purchasing scheme, we have created an absolutely safe environment and our XDR-Analyst Exam Question are free of virus attack. If there is any doubt about it, professional personnel will handle this at first time, and you can also have their remotely online guidance to install and use our XDR-Analyst test torrent.

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	• 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 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 Latest Test Dumps <<

Exam Palo Alto Networks XDR-Analyst Guide Materials | Valid XDR-Analyst Exam Prep

Just as I have just mentioned, almost all of our customers have passed the exam as well as getting the related certification easily with the help of our XDR-Analyst Exam Torrent, we strongly believe that it is impossible for you to be the exception. So choosing our Palo Alto Networks XDR Analyst exam question actually means that you will have more opportunities to get promotion in the near future, at the same time, needless to say that you will get a raise in pay accompanied with the promotion. What's more, when you have shown your talent with Palo Alto Networks XDR Analyst certification in relating field, naturally, you will have the chance to enlarge your friends circle with a lot of distinguished persons who may influence you career life profoundly.

Palo Alto Networks XDR Analyst Sample Questions (Q78-Q83):

NEW QUESTION # 78
Which of the following Live Terminal options are available for Android systems?

- A. Live Terminal is not supported.
- B. Run Android commands.
- C. Run APK scripts.
- D. Stop an app.

Answer: B

Explanation:
Cortex XDR supports Live Terminal for Android systems, which allows you to remotely access and manage Android endpoints using a command-line interface. You can use Live Terminal to run Android commands, such as adb shell, adb logcat, adb install, and adb uninstall. You can also use Live Terminal to view and modify files, directories, and permissions on the Android endpoints. Live Terminal for Android systems does not support stopping an app or running APK scripts. Reference:
Cortex XDR documentation portal
Initiate a Live Terminal Session
Live Terminal Commands

NEW QUESTION # 79
When is the wss (WebSocket Secure) protocol used?

- A. when the Cortex XDR agent uploads alert data
- B. when the Cortex XDR agent establishes a bidirectional communication channel
- C. when the Cortex XDR agent downloads new security content
- D. when the Cortex XDR agent connects to WildFire to upload files for analysis

Answer: B

Explanation:
The WSS (WebSocket Secure) protocol is an extension of the WebSocket protocol that provides a secure communication channel over the internet. It is used to establish a persistent, full-duplex communication channel between a client (in this case, the Cortex XDR agent) and a server (such as the Cortex XDR management console or other components). The Cortex XDR agent uses the WSS protocol to establish a secure and real-time bidirectional communication channel with the Cortex XDR management console or other components in the Palo Alto Networks security ecosystem. This communication channel allows the agent to send data, such as security events, alerts, and other relevant information, to the management console, and receive commands, policy updates, and responses in return. By using the WSS protocol, the Cortex XDR agent can maintain a persistent connection with the management console, which enables timely communication of security-related information and allows for efficient incident response and

remediation actions. It's important to note that the other options mentioned in the question also involve communication between the Cortex XDR agent and various components, but they do not specifically mention the use of the WSS protocol. For example:
A . The Cortex XDR agent downloading new security content typically utilizes protocols like HTTP or HTTPS.
B . When the Cortex XDR agent uploads alert data, it may use protocols like HTTP or HTTPS to transmit the data securely.
C . When the Cortex XDR agent connects to WildFire to upload files for analysis, it typically uses protocols like HTTP or HTTPS.
Therefore, the correct answer is D, when the Cortex XDR agent establishes a bidirectional communication channel. Reference:
Device communication protocols - AWS IoT Core
WebSocket - Wikipedia
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) - Palo Alto Networks
[What are WebSockets? | Web Security Academy]
[Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification exam practice question and answer (Q&A) dump with detail explanation and reference available free, helpful to pass the Palo Alto Networks Certified Detection and Remediation Analyst PCDRA exam and earn Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification.]

NEW QUESTION # 80
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

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

Answer: A,B

NEW QUESTION # 81
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 # 82
What is the outcome of creating and implementing an alert exclusion?

- A. The Cortex XDR console will hide those alerts.
- B. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.
- C. The Cortex XDR agent will not create an alert for this event in the future.
- D. The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Answer: A

Explanation:
The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint. Therefore, the correct answer is B, the Cortex XDR console will hide those alerts12 Reference:
Alert Exclusions
Create an Alert Exclusion Policy

NEW QUESTION # 83
.....

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, myportal.utt.edu.tt, Disposable vapes