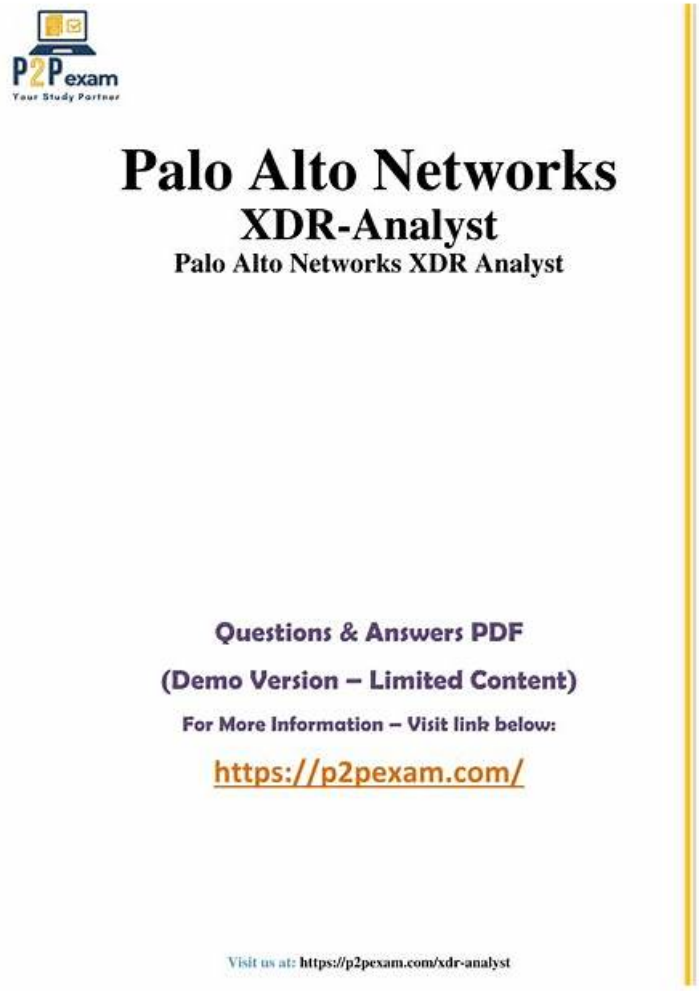
Free PDF Quiz 2026 Palo Alto Networks XDR-Analyst: High Hit-Rate Palo Alto Networks XDR Analyst Certification Practice



We declare that we can ensure you 100% pass, because we have the real exam questions for the XDR-Analyst actual test. All the questions of Palo Alto Networks XDR-Analyst test pdf are taken from current pool of actual test, then after refined and checked, compiled into the complete dumps. Furthermore, the answers are correct and verified by our IT experts with decades of hands-on experience. So the high quality and accuracy of XDR-Analyst Cert Guide are without any doubt. With our 100 % pass rate history & money back guarantee, you can rest assured to choose our XDR-Analyst vce files.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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.

>> XDR-Analyst Certification Practice <<

2026 XDR-Analyst Certification Practice - The Best Palo Alto Networks XDR-Analyst Reliable Test Camp: Palo Alto Networks XDR Analyst

BraindumpsPass is a trusted platform that is committed to helping Palo Alto Networks XDR-Analyst exam candidates in exam preparation. The Palo Alto Networks XDR-Analyst exam questions are real and updated and will repeat in the upcoming Palo Alto Networks XDR-Analyst Exam Dumps. By practicing again and again you will become an expert to solve all the Palo Alto Networks XDR-Analyst exam questions completely and before the exam time.

Palo Alto Networks XDR Analyst Sample Questions (Q60-Q65):

NEW QUESTION # 60
Which statement is correct based on the report output below?

- A. 133 agents have full disk encryption.
- B. 3,297 total incidents have been detected.
- C. Forensic inventory data collection is enabled.
- D. Host Inventory Data Collection is enabled.

Answer: C

Explanation:
The report output shows the number of endpoints that have forensic inventory data collection enabled, which is a feature of Cortex XDR that allows the collection of detailed information about the endpoint's hardware, software, and network configuration. This feature helps analysts to investigate and respond to incidents more effectively by providing a comprehensive view of the endpoint's state and activity. Forensic inventory data collection can be enabled or disabled per policy in Cortex XDR. Reference:
Forensic Inventory Data Collection
Cortex XDR 3: Getting Started with Endpoint Protection

NEW QUESTION # 61
Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

- A. Incident Management Dashboard
- B. Security Manager Dashboard
- C. Data Ingestion Dashboard
- D. Security Admin Dashboard

Answer: A

Explanation:
The Incident Management Dashboard provides a high-level overview of the incident response process, including the Mean Time to Resolution (MTTR) metric. This metric measures the average time it takes to resolve an incident from the moment it is created to the moment it is closed. The dashboard also shows the number of incidents by status, severity, and assigned analyst, as well as the top alerts by category, source, and destination. The Incident Management Dashboard is designed for executives and managers who want to monitor the performance and efficiency of their security teams. Reference: [PCDRA Study Guide], page 18.

NEW QUESTION # 62
What should you do to automatically convert leads into alerts after investigating a lead?

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

Answer: C

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 # 63
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 connects to WildFire to upload files for analysis
- D. when the Cortex XDR agent downloads new security content

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 # 64
You can star security events in which two ways? (Choose two.)

- A. Create an Incident-starring configuration.
- B. Manually star an alert.
- C. Manually star an Incident.
- D. Create an alert-starring configuration.

Answer: B,C

Explanation:
You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you prioritize and track the events that are most important to you. You can also filter and sort the events by their star status in the Cortex XDR console.
To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again.
To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed.
Reference:
Star Security Events
Create an Alert Starring Configuration
Create an Incident Starring Configuration

NEW QUESTION # 65
.....

PDF

- XDR-Analyst Valid Exam Braindumps □ Pass XDR-Analyst Test □ XDR-Analyst Latest Test Experience □ Download ➡ XDR-Analyst □□□ for free by simply searching on ➤ www.prepawayete.com □ □Latest XDR-Analyst Exam Fee
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, Disposable vapes