XDR-Analyst Exam Sample Questions | XDR-Analyst Reliable Source

P.S. Free 2026 Palo Alto Networks XDR-Analyst dumps are available on Google Drive shared by PDF4Test: https://drive.google.com/open?id=1Y3mja-ubKABgaKp7ZMaYBj39OFSop5GR

While making revisions and modifications to the Palo Alto Networks XDR-Analyst practice exam, our team takes reports from over 90,000 professionals worldwide to make the Palo Alto Networks XDR Analyst exam questions foolproof. To make you capable of preparing for the Palo Alto Networks XDR-Analyst Exam smoothly, we provide actual Palo Alto Networks XDR-Analyst exam dumps.

If you start to prapare for the XDR-Analyst exam from books, then you will find that the content is too broad for you to cope with the exam questions. So, we just pick out the most important knowledge to learn. Through large numbers of practices, you will soon master the core knowledge of the XDR-Analyst Exam. It is important to review the questions you always choose mistakenly. You should concentrate on finishing all exercises once you are determined to pass the XDR-Analyst exam. And you will pass for sure as long as you study with our XDR-Analyst study guide carefully.

>> XDR-Analyst Exam Sample Questions <<

XDR-Analyst Reliable Source & XDR-Analyst Exam Preview

PDF4Test also offers you a demo version of the XDR-Analyst exam dumps. Often XDR-Analyst test takers run on a tight budget so they just can not risk wasting it on invalid Palo Alto Networks XDR-Analyst Study Materials. Thus PDF4Test offers a demo version of Palo Alto Networks XDR-Analyst actual exam questions before buying it.

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	• 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 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.

Palo Alto Networks XDR Analyst Sample Questions (Q79-Q84):

NEW QUESTION # 79
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

- A. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
- B. Enable DLL Protection on all servers but there might be some false positives.
- C. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- D. Create IOCs of the malicious files you have found to prevent their execution.

Answer: C

Explanation:
To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted3.
C . Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection4.
D . Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not have an option to enable or configure BTP rules.
In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply chain attack.
Reference:
Behavioral Threat Protection
Create a BTP Rule
DLL Protection
Create an IOC Rule
[Cytool]

NEW QUESTION # 80

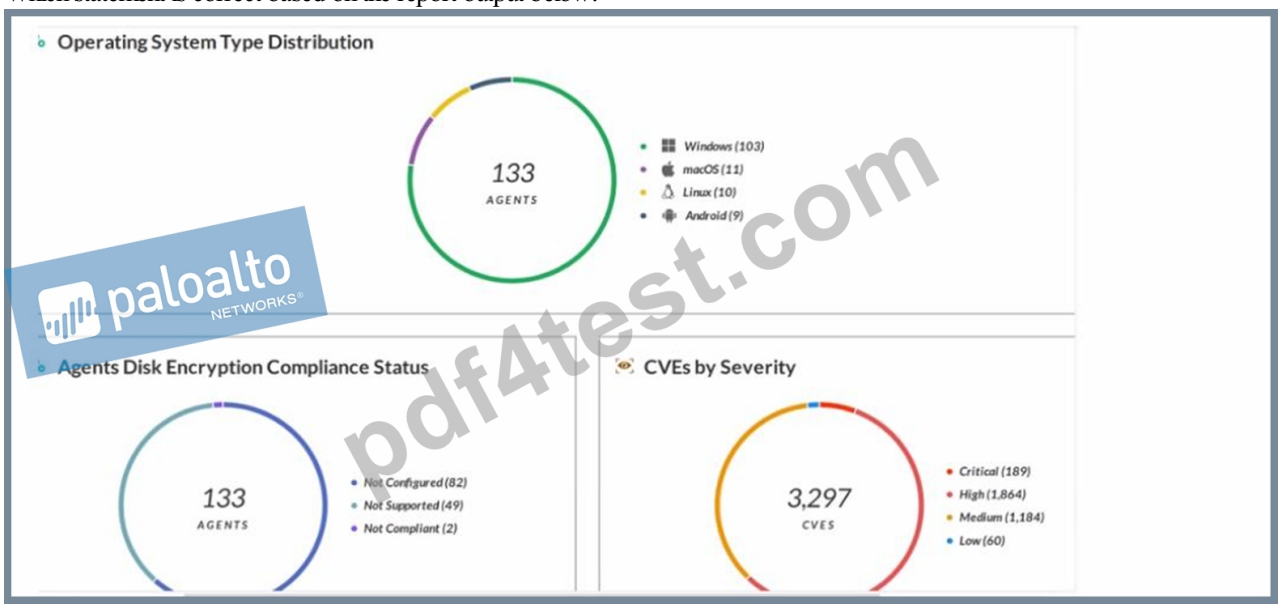
Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

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

Answer: C

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 # 81
Which statement is correct based on the report output below?



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

Answer: B

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 # 82
How can you pivot within a row to Causality view and Timeline views for further investigate?

- A. Using Open Timeline Actions Only
- B. You can't pivot within a row to Causality view and Timeline views

- C. Using the Open Card Only
- D. Using the Open Card and Open Timeline actions respectively

Answer: D

Explanation:
To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident. Reference:
Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

NEW QUESTION # 83
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. Search & destroy
- B. Flag for removal
- C. Quarantine
- D. Isolation

Answer: C

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 # 84
.....

- XDR-Analyst Reliable Exam Prep □ XDR-Analyst Latest Test Questions □ XDR-Analyst Exam Blueprint □ Enter 《 www.pdfvce.com 》 and search for { XDR-Analyst } to download for free □Valid XDR-Analyst Practice Materials
- XDR-Analyst Reliable Exam Prep □ XDR-Analyst Latest Test Questions □ XDR-Analyst Pass Exam □ Enter " www.validtorrent.com " and search for ➤ XDR-Analyst □ to download for free □Latest XDR-Analyst Exam Answers
- XDR-Analyst Test Torrent and XDR-Analyst Preparation Materials: Palo Alto Networks XDR Analyst - XDR-Analyst Practice Test □ Download ➡ XDR-Analyst □□□ for free by simply searching on ➥ www.pdfvce.com □ □XDR-Analyst Guide Torrent
- 2026 RealisticXDR-Analyst Reliable Source - Palo Alto Networks Palo Alto Networks XDR Analyst Exam Sample Questions 100% Pass □ Search on ⇛ www.torrentvce.com ⇚ for ➥ XDR-Analyst □ to obtain exam materials for free download □Testking XDR-Analyst Exam Questions
- 2026 RealisticXDR-Analyst Reliable Source - Palo Alto Networks Palo Alto Networks XDR Analyst Exam Sample Questions 100% Pass □ Search for □ XDR-Analyst □ and download exam materials for free through ➡ www.pdfvce.com □□□ ↕XDR-Analyst Updated Testkings
- 2026 Palo Alto Networks XDR-Analyst: Trustable Palo Alto Networks XDR Analyst Exam Sample Questions □ Search for ➥ XDR-Analyst □ and easily obtain a free download on { www.examcollectionpass.com } □Practice XDR-Analyst Engine
- chiaracdxa278918.thelateblog.com, fanniehglv716300.wikifordummies.com, iwannpwm754810.wikilinksnews.com, nanniepseg021218.gigswiki.com, minaytgj134106.idblogmaker.com, liviaomxi928569.wikigop.com, matheeriq137309.blog-gold.com, shaniasizc253752.plpwiki.com, poppylyxy989769.blog-kids.com, leftbookmarks.com, Disposable vapes

BTW, DOWNLOAD part of PDF4Test XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1Y3mja-ubKABgaKp7ZMaYBj39OFSop5GR