Latest XDR-Analyst Braindumps Files & New XDR-Analyst Test Braindumps

What's more, part of that Prep4sureExam XDR-Analyst dumps now are free: https://drive.google.com/open?id=1DAcY7wc3gDzaqtF8893cyapQhzC6-LYR

To solve all these problems, Prep4sureExam offers actual XDR-Analyst Questions to help candidates overcome all the obstacles and difficulties they face during XDR-Analyst examination preparation. With vast experience in this field, Prep4sureExam always comes forward to provide its valued customers with authentic, actual, and genuine XDR-Analyst Exam Dumps at an affordable cost. All the Palo Alto Networks XDR Analyst (XDR-Analyst) questions given in the product are based on actual examination topics.

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.

New XDR-Analyst Test Braindumps - New XDR-Analyst Exam Questions

We have a lasting and sustainable cooperation with customers who are willing to purchase our XDR-Analyst actual exam. We try our best to renovate and update our XDR-Analyst study materials in order to help you fill the knowledge gap during your learning process, thus increasing your confidence and success rate. At the same time, XDR-Analyst Preparation baindumps can keep pace with the digitized world by providing timely application. You will never fell disappointed with our XDR-Analyst exam quiz.

Palo Alto Networks XDR Analyst Sample Questions (Q89-Q94):

NEW QUESTION # 89
How can you pivot within a row to Causality view and Timeline views for further investigate?

- A. Using Open Timeline Actions Only
- B. Using the Open Card and Open Timeline actions respectively
- C. You can't pivot within a row to Causality view and Timeline views
- D. Using the Open Card Only

Answer: B

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 # 90
Which statement best describes how Behavioral Threat Protection (BTP) works?

- A. BTP matches EDR data with rules provided by Cortex XDR.
- B. BTP uses machine Learning to recognize malicious activity even if it is not known.
- C. BTP injects into known vulnerable processes to detect malicious activity.
- D. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

Answer: B

Explanation:
The statement that best describes how Behavioral Threat Protection (BTP) works is D, BTP uses machine learning to recognize malicious activity even if it is not known. BTP is a feature of Cortex XDR that allows you to define custom rules to detect and block malicious behaviors on endpoints. BTP uses machine learning to profile behavior and detect anomalies indicative of attack. BTP can recognize malicious activity based on file attributes, registry keys, processes, network connections, and other criteria, even if the activity is not associated with any known malware or threat. BTP rules are updated through content updates and can be managed from the Cortex XDR console.
The other statements are incorrect for the following reasons:
A is incorrect because BTP does not inject into known vulnerable processes to detect malicious activity. BTP does not rely on

process injection, which is a technique used by some malware to hide or execute code within another process. BTP monitors the behavior of all processes on the endpoint, regardless of their vulnerability status, and compares them with the BTP rules.
B is incorrect because BTP does not run on the Cortex XDR and distribute behavioral signatures to all agents. BTP runs on the Cortex XDR agent, which is installed on the endpoint, and analyzes the endpoint data locally. BTP does not use behavioral signatures, which are predefined patterns of malicious behavior, but rather uses machine learning to identify anomalies and deviations from normal behavior.
C is incorrect because BTP does not match EDR data with rules provided by Cortex XDR. BTP is part of the EDR (Endpoint Detection and Response) capabilities of Cortex XDR, and uses the EDR data collected by the Cortex XDR agent to perform behavioral analysis. BTP does not match the EDR data with rules provided by Cortex XDR, but rather applies the BTP rules defined by the Cortex XDR administrator or the Palo Alto Networks threat research team.
Reference:
Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR: Stop Breaches with AI-Powered Cybersecurity

NEW QUESTION # 91
Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

- A. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.
- B. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.
- C. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.
- D. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.

Answer: C

Explanation:
To add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint, you need to use the Action Center in Cortex XDR. The Action Center allows you to create and manage actions that apply to endpoints, such as adding files or processes to the allow list or block list, isolating or unisolating endpoints, or initiating live terminal sessions. To add a file hash to the allow list, you need to choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it. This will prevent the Malware profile from scanning or blocking the file on the endpoints that match the scope of the action.
Reference: Cortex XDR 3: Responding to Attacks1, Action Center2

NEW QUESTION # 92
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

- A. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.
- B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- C. No step is required because the malicious document is already stopped.
- D. Enable DLL Protection on all endpoints but there might be some false positives.

Answer: B

Explanation:
The correct answer is B, create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP rules are a powerful feature of Cortex XDR that allow you to define custom rules to detect and block malicious behaviors on endpoints. You can use BTP rules to create indicators of compromise (IOCs) based on file attributes, registry keys, processes, network connections, and other criteria. By creating BTP rules, you can prevent the same malicious Word document from being opened by other users in your organization, even if the document has a different name or hash value. BTP rules are updated through content updates and can be managed from the Cortex XDR console.
The other options are incorrect for the following reasons:
A is incorrect because enabling DLL Protection on all endpoints is not a specific or effective way to prevent the malicious Word document. DLL Protection is a feature of Cortex XDR that prevents the loading of unsigned or untrusted DLLs by protected processes. However, this feature does not apply to Word documents or macros, and may cause false positives or compatibility

issues with legitimate applications.
C is incorrect because relying on Cortex to share IOCs with the Cyber Threat Alliance members is not a proactive or sufficient way to prevent the malicious Word document. The Cyber Threat Alliance is a group of cybersecurity vendors that share threat intelligence and best practices to improve their products and services. However, not all vendors are members of the alliance, and not all IOCs are shared or updated in a timely manner. Therefore, you cannot assume that other users in your organization are protected by the same IOCs as Cortex XDR.
D is incorrect because doing nothing is not a responsible or secure way to prevent the malicious Word document. Even though Cortex XDR agent prevented the attempt to open the document on one endpoint, it does not mean that the document is no longer a threat. The document may still be circulating in your network or email system, and may be opened by other users who have different agent profiles or policies. Therefore, you should take steps to identify and block the document across your organization.
Reference:
Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR Agent Administrator Guide: DLL Protection
Palo Alto Networks: Cyber Threat Alliance

NEW QUESTION # 93
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

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

Answer: B,C

NEW QUESTION # 94
.....

We offer free demos and updates if there are any for your reference beside real XDR-Analyst real materials. By downloading the free demos you will catch on the basic essences of our XDR-Analyst guide question and just look briefly at our practice materials you can feel the thoughtful and trendy of us. About difficult or equivocal points, our experts left notes to account for them. So XDR-Analyst Exam Dumps are definitely valuable acquisitions. Wrong practice materials will upset your pace of review, which is undesirable. Only high-class XDR-Analyst guide question like us can be your perfect choice.

XDR-Analyst] by searching on 【 www.pdfvce.com 】 □Valid Exam XDR-Analyst Vce Free

- Expertly-Researched Palo Alto Networks XDR-Analyst PDF Questions from www.prepawayete.com □ Download [XDR-Analyst] for free by simply searching on ➥ www.prepawayete.com □ □Valid Exam XDR-Analyst Vce Free
- henrigprs465986.tkzblog.com, jeanokot269866.therainblog.com, ianvizc261946.snack-blog.com, shopwebdirectory.com, 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, bookmarksusa.com, steverzlb972123.blogaritma.com, natural-bookmark.com, mattiebfhv572907.national-wiki.com, digitalwbl.com, Disposable vapes

P.S. Free 2026 Palo Alto Networks XDR-Analyst dumps are available on Google Drive shared by Prep4sureExam: https://drive.google.com/open?id=1DAcY7wc3gDzaqtF8893cyapQhzC6-LYR