XDR-Analyst Latest Test Preparation, XDR-Analyst Certification Test Questions

To keep pace with the times, we believe science and technology can enhance the way people study on our XDR-Analyst exam materials. Especially in such a fast-pace living tempo, we attach great importance to high-efficient learning our XDR-Analyst Study Guide. Therefore, our XDR-Analyst study materials base on the past exam papers and the current exam tendency, and design such an effective simulation function to place you in the real exam environment.

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	- 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 3	- 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 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 Preparation <<

XDR-Analyst Certification Test Questions, XDR-Analyst Reliable Exam Tutorial

Perhaps you worry about the quality of our XDR-Analyst exam questions. We can make solemn commitment that our XDR-Analyst study materials have no mistakes. All contents are passing rigid inspection. You will never find small mistakes such as spelling mistakes and typographical errors in our XDR-Analyst learning guide. No one is willing to buy a defective product. And our XDR-Analyst practice braindumps are easy to understand for all the candidates.

Palo Alto Networks XDR Analyst Sample Questions (Q11-Q16):

NEW QUESTION # 11
What is the outcome of creating and implementing an alert exclusion?

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

Answer: B

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 # 12
Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?

- A. Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.
- B. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.
- C. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.
- D. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

Answer: D

Explanation:
Cortex XDR Analytics is a cloud-based service that uses machine learning and artificial intelligence to detect and prevent network attacks. Cortex XDR Analytics can interfere with the attack pattern as soon as it is observed on the endpoint by applying protection policies that block malicious processes, files, or network connections. This way, Cortex XDR Analytics can stop the attack before it causes any damage or compromises the system. Reference:
[Cortex XDR Analytics Overview]
[Cortex XDR Analytics Protection Policies]

NEW QUESTION # 13
Why would one threaten to encrypt a hypervisor or, potentially, a multiple number of virtual machines running on a server?

- A. To potentially perform a Distributed Denial of Attack.
- B. To better understand the underlying virtual infrastructure.

- C. To gain notoriety and potentially a consulting position.
- D. To extort a payment from a victim or potentially embarrass the owners.

Answer: D

Explanation:
Encrypting a hypervisor or a multiple number of virtual machines running on a server is a form of ransomware attack, which is a type of cyberattack that involves locking or encrypting the victim's data or system and demanding a ransom for its release. The attacker may threaten to encrypt the hypervisor or the virtual machines to extort a payment from the victim or potentially embarrass the owners by exposing their sensitive or confidential information. Encrypting a hypervisor or a multiple number of virtual machines can have a severe impact on the victim's business operations, as it can affect the availability, integrity, and confidentiality of their data and applications. The attacker may also use the encryption as a leverage to negotiate a higher ransom or to coerce the victim into complying with their demands. Reference:
Encrypt an Existing Virtual Machine or Virtual Disk: This document explains how to encrypt an existing virtual machine or virtual disk using the vSphere Client.
How to Encrypt an Existing or New Virtual Machine: This article provides a guide on how to encrypt an existing or new virtual machine using AOMEI Backupper.
Ransomware: This document provides an overview of ransomware, its types, impacts, and prevention methods.

NEW QUESTION # 14
When creating a BIOC rule, which XQL query can be used?

- A. dataset = xdr_data
  | filter event_behavior = true
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- B. dataset = xdr_data
  | filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
  | fields action_process_image
- C. dataset = xdr_data
  | filter event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- D. dataset = xdr_data
  | filter event_type = PROCESS and
  event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Answer: D

Explanation:
A BIOC rule is a custom detection rule that uses the Cortex Query Language (XQL) to define the behavior or actions that indicate a potential threat. A BIOC rule can use the xdr_data and cloud_audit_log datasets and presets for these datasets. A BIOC rule can also use the filter stage, alter stage, and functions without any aggregations in the XQL query. The query must return a single field named action_process_image, which is the process image name of the suspicious process. The query must also include the event_type and event_sub_type fields in the filter stage to specify the type and sub-type of the event that triggers the rule.
Option B is the correct answer because it meets all the requirements for a valid BIOC rule query. It uses the xdr_data dataset, the filter stage, the event_type and event_sub_type fields, and the action_process_image_name field with a regular expression to match any process image name that ends with .pdf.exe or .docx.exe, which are common indicators of malicious files.
Option A is incorrect because it does not include the event_type field in the filter stage, which is mandatory for a BIOC rule query.
Option C is incorrect because it does not include the event_type and event_sub_type fields in the filter stage, and it uses the fields stage, which is not supported for a BIOC rule query. It also returns the action_process_image field instead of the action_process_image_name field, which is the expected output for a BIOC rule query.
Option D is incorrect because it uses the event_behavior field, which is not supported for a BIOC rule query. It also does not include the event_type field in the filter stage, and it uses the event_sub_type field incorrectly. The event_sub_type field should be equal to PROCESS_START, not true.
Reference:
Working with BIOCs
Cortex Query Language (XQL) Reference

NEW QUESTION # 15
Where would you view the WildFire report in an incident?

- A. on the HUB page at apps.paloaltonetworks.com
- B. under the gear icon --> Agent Audit Logs
- C. next to relevant Key Artifacts in the incidents details page
- D. under Response --> Action Center

Answer: C

Explanation:
To view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. A key artifact is a piece of evidence that is associated with an alert or an incident, such as a file hash, a registry key, an IP address, a domain name, or a full path. If a key artifact is related to a WildFire analysis, you will see a WildFire icon next to it, indicating that there is a WildFire report available for that artifact. You can click on the WildFire icon to view the report, which will show you the detailed information about the artifact, such as the verdict, the behavior, the severity, the signatures, and the screenshots12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . under Response --> Action Center: This is not the correct answer. The Action Center is a feature that allows you to create and manage actions that you can perform on your endpoints, such as isolating, scanning, collecting files, or executing scripts. The Action Center does not show you the WildFire reports for the incidents, but it can help you to remediate the incidents by applying the appropriate actions3.
C . under the gear icon --> Agent Audit Logs: This is not the correct answer. The Agent Audit Logs are logs that show you the activities and events that occurred on the Cortex XDR agents, such as installation, upgrade, connection, policy update, or prevention. The Agent Audit Logs do not show you the WildFire reports for the incidents, but they can help you to troubleshoot the agent issues or verify the agent status4.
D . on the HUB page at apps.paloaltonetworks.com: This is not the correct answer. The HUB page is a web portal that allows you to access and manage your Palo Alto Networks applications, such as Cortex XDR, Cortex XSOAR, Prisma Cloud, or AutoFocus. The HUB page does not show you the WildFire reports for the incidents, but it can help you to navigate to the different applications or view the notifications and alerts5.
In conclusion, to view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. By viewing the WildFire report, you can gain more insights and context about the incident and the artifact.
Reference:
View Incident Details
View WildFire Reports
Action Center
Agent Audit Logs
HUB

NEW QUESTION # 16
......

To avail of all these Palo Alto Networks XDR-Analyst certification exam benefits you need to enroll in Palo Alto Networks XDR-Analyst certification exam and pass it with good scores. Are you ready for this? If your answer is right then you do not need to go anywhere. Just download Palo Alto Networks XDR-Analyst Dumps questions and start preparing today.

XDR-Analyst Certification Test Questions: https://www.latestcram.com/XDR-Analyst-exam-cram-questions.html

- Valid XDR-Analyst Study Notes □ Valid XDR-Analyst Study Notes □ XDR-Analyst Valid Exam Online □ Search for ✔ XDR-Analyst □✔□ and download it for free on { www.vce4dumps.com } website □Latest XDR-Analyst Exam Tips
- XDR-Analyst New Exam Braindumps □ XDR-Analyst Paper □ XDR-Analyst Exam Cram Pdf □ Go to website □ www.pdfvce.com □ open and search for ➠ XDR-Analyst □ to download for free □Exam Dumps XDR-Analyst Collection
- XDR-Analyst Exam Flashcards □ XDR-Analyst Exam Flashcards □ XDR-Analyst New Cram Materials ✔ Open website ✔ www.troytecdumps.com □✔□ and search for 「 XDR-Analyst 」 for free download □XDR-Analyst New Dumps Pdf
- Ace Your Exam Preparation with Pdfvce Palo Alto Networks XDR-Analyst PDF Dumps □ Enter ▹ www.pdfvce.com ◃ and search for { XDR-Analyst } to download for free □XDR-Analyst Sample Questions
- Free PDF 2026 Palo Alto Networks Marvelous XDR-Analyst: Palo Alto Networks XDR Analyst Latest Test Preparation □

□ Immediately open ➽ www.dumpsquestion.com □ and search for □ XDR-Analyst □ to obtain a free download □ □Most XDR-Analyst Reliable Questions

- XDR-Analyst Paper □ Exams XDR-Analyst Torrent □ XDR-Analyst Exam Flashcards □ Simply search for ➽ XDR-Analyst □ for free download on “ www.pdfvce.com ” □XDR-Analyst Reliable Dump
- Latest XDR-Analyst Exam Tips □ XDR-Analyst Exam Flashcards □ Exams XDR-Analyst Torrent □ Open website （ www.exam4labs.com ） and search for 【 XDR-Analyst 】 for free download □Latest XDR-Analyst Exam Tips
- XDR-Analyst New Exam Braindumps □ XDR-Analyst New Exam Braindumps □ Exam Dumps XDR-Analyst Collection □ Go to website ➽ www.pdfvce.com □ open and search for □ XDR-Analyst □ to download for free □XDR-Analyst New Cram Materials
- 100% Pass Palo Alto Networks - Useful XDR-Analyst Latest Test Preparation □ Easily obtain free download of ➥ XDR-Analyst □ by searching on ➽ www.vce4dumps.com □ □Most XDR-Analyst Reliable Questions
- XDR-Analyst Paper □ XDR-Analyst Pass Test Guide □ Latest XDR-Analyst Exam Tips □ Search for ▶ XDR-Analyst ◀ on （ www.pdfvce.com ） immediately to obtain a free download □Valid XDR-Analyst Study Notes
- XDR-Analyst Paper □ Most XDR-Analyst Reliable Questions □ Exam Dumps XDR-Analyst Collection ➡ The page for free download of □ XDR-Analyst □ on 《 www.examcollectionpass.com 》 will open immediately □XDR-Analyst Exam Flashcards
- www.stes.tyc.edu.tw, k12.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, carrigrow.com, 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, Disposable vapes