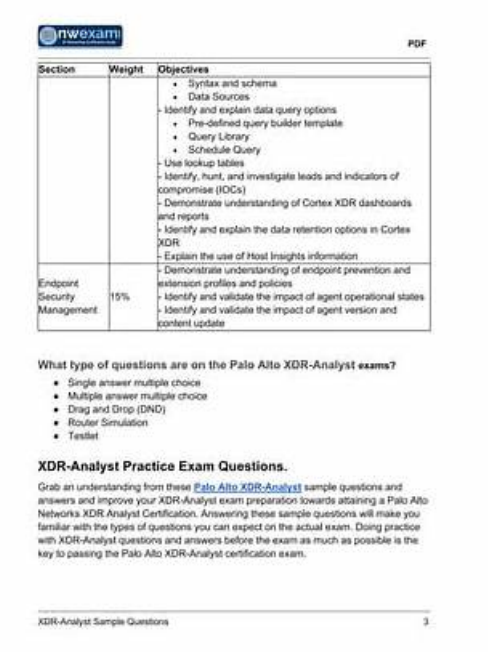
Pass XDR-Analyst Exam with Authoritative Valid XDR-Analyst Test Camp by VCEPrep



nwexam

PDF

Section	Weight	Objectives
		• Syntax and schema • Data Sources - Identify and explain data query options • Pre-defined query builder template • Query Library • Schedule Query - Use lookup tables - Identify, hunt, and investigate leads and indicators of compromise (IOCs) - Demonstrate understanding of Cortex XDR dashboards and reports - Identify and explain the data retention options in Cortex XDR - Explain the use of Host Insights information
Endpoint Security Management	15%	- Demonstrate understanding of endpoint prevention and extension profiles and policies - Identify and validate the impact of agent operational states - Identify and validate the impact of agent version and content update

What type of questions are on the Palo Alto XDR-Analyst exams?

- Single answer multiple choice
- Multiple answer multiple choice
- Drag and Drop (DND)
- Router Simulation
- Testlet

XDR-Analyst Practice Exam Questions.

Grab an understanding from these Palo Alto XDR-Analyst sample questions and answers and improve your XDR-Analyst exam preparation towards attaining a Palo Alto Networks XDR Analyst Certification. Answering these sample questions will make you familiar with the types of questions you can expect on the actual exam. Doing practice with XDR-Analyst questions and answers before the exam as much as possible is the key to passing the Palo Alto XDR-Analyst certification exam.

XDR-Analyst Sample Questions 3

BONUS!!! Download part of VCEPrep XDR-Analyst dumps for free: https://drive.google.com/open?id=1lEfLFeZF_GT8zUDpYFu9GIZ00ippDXOg

As you know, many exam and tests depend on the skills rather than knowledge solely. Our XDR-Analyst exam materials are time-tested materials for your information. There are free demos of our XDR-Analyst training guide for your reference with brief catalogue and outlines in them. For a XDR-Analyst study engine develop to full maturity, it is rewarding and hard. And we have engaged for more than ten years and successfully make every detail of our XDR-Analyst practice braindumps to be perfect.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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.

Testking XDR-Analyst Learning Materials - XDR-Analyst Latest Exam Testking

The quality of the XDR-Analyst exam product is very important. A high-quality XDR-Analyst exam study material can save your time spent on the study and can also enhance your confidence. Here, our Palo Alto Networks XDR-Analyst exam vce dumps will be the right study material for you. XDR-Analyst Training Pdf cannot only help you pass your exam, but also widen your horizons. Then passing the XDR-Analyst exam test is a certain thing. Equipped with the skills of XDR-Analyst certification, you will have more opportunity in your career.

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

NEW QUESTION # 60
Phishing belongs to which of the following MITRE ATT&CK tactics?

- A. Reconnaissance, Initial Access
- B. Reconnaissance, Persistence
- C. Initial Access, Persistence
- D. Persistence, Command and Control

Answer: A

Explanation:
Phishing is a technique that belongs to two MITRE ATT&CK tactics: Reconnaissance and Initial Access. Reconnaissance is the process of gathering information about a target before launching an attack. Phishing for information is a sub-technique of Reconnaissance that involves sending phishing messages to elicit sensitive information that can be used during targeting. Initial Access is the process of gaining a foothold in a network or system. Phishing is a sub-technique of Initial Access that involves sending phishing messages to execute malicious code on victim systems. Phishing can be used for both Reconnaissance and Initial Access depending on the objective and content of the phishing message. Reference:
Phishing, Technique T1566 - Enterprise | MITRE ATT&CK 1
Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK 2 Phishing for information, Part 2: Tactics and techniques 3 PHISHING AND THE MITREATT&CK FRAMEWORK - EnterpriseTalk 4 Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK 5

NEW QUESTION # 61
When creating a BIOC rule, which XQL query can be used?

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

action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

- D. dataset = xdr_data
  | filter event_sub_type = PROCESS_START and
  action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Answer: C

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 # 62
In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

- A. Create a new rule exception and use the singer as the characteristic.
- B. In the Restrictions Profile, add the file name and path to the Executable Files allow list.
- C. Add the signer to the allow list under the action center page.
- D. Add the signer to the allow list in the malware profile.

Answer: D

Explanation:
To prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. A malware profile is a profile that defines the settings and actions for malware prevention and detection on the endpoints. A malware profile allows you to specify a list of files, folders, or signers that you want to exclude from malware scanning and blocking. By adding the signer to the allow list in the malware profile, you can prevent the Cortex XDR Agent from blocking any file that is signed by that signer1.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . In the Restrictions Profile, add the file name and path to the Executable Files allow list: This is not the correct answer. Adding the file name and path to the Executable Files allow list in the Restrictions Profile will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A Restrictions Profile is a profile that defines the settings and actions for restricting the execution of files or processes on the endpoints. A Restrictions Profile allows you to specify a list of executable files that you want to allow or block based on the file name and path. However, this method does not take into account the digital signer of the file, and it may not be effective if the file name or path changes2.
B . Create a new rule exception and use the signer as the characteristic: This is not the correct answer. Creating a new rule exception and using the signer as the characteristic will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A rule exception is an exception that you can create to modify the behavior of a specific prevention rule or BIOC rule. A rule exception allows you to specify the characteristics and the actions that you want to apply to the exception, such as file hash, process name, IP address, or domain name. However, this method does not support using the signer as a characteristic, and it may not be applicable to all prevention rules or BIOC rules3.
D . Add the signer to the allow list under the action center page: This is not the correct answer. Adding the signer to the allow list under the action center page will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. The action center page is a page 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 page does not have an option to add a signer to the allow list, and it is not related to the malware prevention or detection functionality4.
In conclusion, to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. By using this method, you can exclude the files that are signed by the trusted signer from the malware scanning and blocking.
Reference:
Add a New Malware Security Profile
Add a New Restrictions Security Profile
Create a Rule Exception
Action Center

NEW QUESTION # 63
What is the standard installation disk space recommended to install a Broker VM?

- A. 2GB disk space
- B. 512GB disk space
- C. 1GB disk space
- D. 256GB disk space

Answer: D

Explanation:
The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location. The system requirements for the Broker VM are as follows:
CPU: 4 cores
RAM: 8 GB
Disk space: 256 GB
Network: Internet access and connectivity to all Cortex XDR agents
The disk space requirement is based on the number of agents and the frequency of content updates. The Broker VM stores the content updates locally and distributes them to the agents. The disk space also depends on the retention period of the content updates, which can be configured in the Broker VM settings. The default retention period is 30 days.
Reference:
Broker VM for Cortex XDR
PCDRA Study Guide

NEW QUESTION # 64
Can you disable the ability to use the Live Terminal feature in Cortex XDR?

- A. Yes, via Agent Settings Profile.
- B. No, a separate installer package without Live Terminal is required.
- C. Yes, via the Cortex XDR console or with an installation switch.
- D. No, it is a required feature of the agent.

Answer: A

Explanation:
The Live Terminal feature in Cortex XDR allows you to initiate a remote connection to an endpoint and perform various actions such as running commands, uploading and downloading files, and terminating processes. You can disable the ability to use the Live Terminal feature in Cortex XDR by configuring the Agent Settings Profile. The Agent Settings Profile defines the behavior and functionality of the Cortex XDR agent on the endpoint. You can create different profiles for different groups of endpoints and assign them accordingly. To disable the Live Terminal feature, you need to uncheck the Enable Live Terminal option in the Agent Settings Profile and save the changes. This will prevent the Cortex XDR agent from accepting any Live Terminal requests from the Cortex XDR management console. Reference:
Live Terminal: This document explains how to use the Live Terminal feature to investigate and respond to security events on Windows endpoints.
Agent Settings Profile: This document describes how to create and manage Agent Settings Profiles to define the behavior and functionality of the Cortex XDR agent on the endpoint.

NEW QUESTION # 65
.....

No matter how good the product is users will encounter some difficult problems in the process of use, and how to deal with these problems quickly becomes a standard to test the level of product service. Our XDR-Analyst real exam materials are not exceptional also, in order to enjoy the best product experience, as long as the user is in use process found any problem, can timely feedback to us, for the first time you check our XDR-Analyst Exam Question performance, professional maintenance staff to help users solve problems. Our XDR-Analyst learning reference files have a high efficient product maintenance team, a professional staff every day real-time monitoring the use of the user environment and learning platform security, even in the incubation period, we can accurate solution for the user, for the use of the user to create a safer environment.

Testking XDR-Analyst Learning Materials: https://www.vceprep.com/XDR-Analyst-latest-vce-prep.html

- 2026 Latest Valid XDR-Analyst Test Camp Help You Pass XDR-Analyst Easily ◂ Search for " XDR-Analyst " and download it for free immediately on □ www.prepawaypdf.com □ □New XDR-Analyst Test Duration
- HOT Valid XDR-Analyst Test Camp: Palo Alto Networks XDR Analyst - Valid Palo Alto Networks Testking XDR-Analyst Learning Materials □ Search for ☀ XDR-Analyst □☀□ and obtain a free download on ▹ www.pdfvce.com ◃ □XDR-Analyst Latest Braindumps Book
- HOT Valid XDR-Analyst Test Camp: Palo Alto Networks XDR Analyst - Valid Palo Alto Networks Testking XDR-Analyst Learning Materials □ Copy URL 【 www.vce4dumps.com 】 open and search for ➥ XDR-Analyst □ to download for free □Valid XDR-Analyst Exam Simulator
- 100% Pass 2026 Palo Alto Networks XDR-Analyst: Palo Alto Networks XDR Analyst –Efficient Valid Test Camp □ Enter ➽ www.pdfvce.com □ and search for □ XDR-Analyst □ to download for free □Reliable XDR-Analyst Dumps
- 2026 Latest Valid XDR-Analyst Test Camp Help You Pass XDR-Analyst Easily ↕ Open website ▹ www.verifieddumps.com ◃ and search for □ XDR-Analyst □ for free download □Reliable XDR-Analyst Dumps
- High-quality Valid XDR-Analyst Test Camp Help You Pass Success Your XDR-Analyst: Palo Alto Networks XDR Analyst Exam Efficiently □ Copy URL ☀ www.pdfvce.com □☀□ open and search for ⇛ XDR-Analyst ⇚ to download for free □Free XDR-Analyst Sample
- Original XDR-Analyst Questions □ Real XDR-Analyst Testing Environment □ XDR-Analyst Latest Exam Pdf □ Download ✔ XDR-Analyst □✔□ for free by simply searching on （ www.prepawaypdf.com ） □Real XDR-Analyst Testing Environment
- HOT Valid XDR-Analyst Test Camp: Palo Alto Networks XDR Analyst - Valid Palo Alto Networks Testking XDR-Analyst Learning Materials □ Search for □ XDR-Analyst □ and download exam materials for free through ▸ www.pdfvce.com ◂ □Reliable XDR-Analyst Dumps
- HOT Valid XDR-Analyst Test Camp: Palo Alto Networks XDR Analyst - Valid Palo Alto Networks Testking XDR-Analyst Learning Materials □ Download " XDR-Analyst " for free by simply entering 《 www.torrentvce.com 》 website □New XDR-Analyst Test Duration
- High-quality Valid XDR-Analyst Test Camp Help You Pass Success Your XDR-Analyst: Palo Alto Networks XDR Analyst Exam Efficiently □ Search for ✔ XDR-Analyst □✔□ and obtain a free download on ▸ www.pdfvce.com ◂ □Latest XDR-Analyst Test Prep
- Free XDR-Analyst Sample □ Latest XDR-Analyst Test Prep □ Valid XDR-Analyst Exam Simulator □ Search for □ XDR-Analyst □ and download it for free on □ www.examcollectionpass.com □ website □Real XDR-Analyst Testing Environment
- fatallisto.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, bookmarksparkle.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, www.tttttt456.com, antonazpx149295.blog2news.com, learn.csisafety.com.au, saadofxb558376.wikiconversation.com, steveomtj887654.blogozz.com, aadamfeeu464602.blogdeazar.com, Disposable vapes

BONUS!!! Download part of VCEPrep XDR-Analyst dumps for free: https://drive.google.com/open?id=1lEfLFeZF_GT8zUDpYFu9GIZ00ippDXOg