Palo Alto Networks XDR-Analyst Exam Dumps - Pass Exam in One Go

In the present society, the workplace is extremely cruel. There is no skill, no certificate, and even if you say it admirably, it is useless. If you want to work, you must get a XDR-Analyst certificate. The certificate is like a stepping stone. It is the key to the unimpeded workplace and the cornerstone of value. And our XDR-Analyst study braindumps will help you pass the exam and get the certification with the least time and effors. Just buy our XDR-Analyst learning question if you want to be successful!

Are you a fresh man in IT industry, or on the way to become an IT career? The XDR-Analyst certification will help you learn professional skills to enhance your personal ability. With our XDR-Analyst test engine, you set the test time as you like. Besides, you can make notes and do marks with XDR-Analyst test engine. With the notes, you will have a clear idea about your XDR-Analyst Exam Preparation. More practice make more perfect, so please take the XDR-Analyst exam preparation seriously. Your dreams will come true if you pass the XDR-Analyst exam certification.Trust Palo Alto Networks XDR-Analyst exam dumps, you will never fail.

>> Exam XDR-Analyst Outline <<

Test XDR-Analyst Guide Online | Latest Braindumps XDR-Analyst Ebook

Our XDR-Analyst preparation exam have assembled a team of professional experts incorporating domestic and overseas experts and scholars to research and design related exam bank, committing great efforts to work for our candidates. Most of the experts have been studying in the professional field for many years and have accumulated much experience in our XDR-Analyst Practice Questions. So we can say that our XDR-Analyst exam questions are the first-class in the market. With our XDR-Analyst learning guide, you will get your certification by your first attempt.

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	- 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 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	- 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.

Palo Alto Networks XDR Analyst Sample Questions (Q69-Q74):

NEW QUESTION # 69
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. Add the signer to the allow list under the action center page.
- B. Create a new rule exception and use the singer as the characteristic.
- C. Add the signer to the allow list in the malware profile.
- D. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

Answer: C

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 singer 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 # 70
How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

- A. by patching vulnerable applications.
- B. by utilizing decoy Files.
- C. by retrieving the encryption key.
- D. by encrypting the disk first.

Answer: B

Explanation:
Cortex XDR agent for Windows prevents ransomware attacks from compromising the file system by utilizing decoy files. Decoy files are randomly generated files that are placed in strategic locations on the endpoint, such as the user's desktop, documents, and pictures folders. These files are designed to look like valuable data that ransomware would target for encryption. When Cortex XDR agent detects that a process is attempting to access or modify a decoy file, it immediately blocks the process and alerts the administrator. This way, Cortex XDR agent can stop ransomware attacks before they can cause any damage to the real files on the endpoint. Reference:
Anti-Ransomware Protection
PCDRA Study Guide

NEW QUESTION # 71
Which of the following represents the correct relation of alerts to incidents?

- A. Every alert creates a new Incident.
- B. Alerts that occur within a three-hour time frame are grouped together into one Incident.
- C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- D. Only alerts with the same host are grouped together into one Incident in a given time frame.

Answer: C

Explanation:
The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details1.
Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.
Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.
Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2 Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

NEW QUESTION # 72
Which profiles can the user use to configure malware protection in the Cortex XDR console?

- A. Malware profile
- B. Malware Protection profile
- C. Anti-Malware profile

- D. Malware Detection profile

Answer: B

Explanation:
The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. Reference:
Malware Protection Profile
Endpoint Security Policy

NEW QUESTION # 73
Which statement regarding scripts in Cortex XDR is true?

- A. Any script can be imported including Visual Basic (VB) scripts.
- B. Any version of Python script can be run.
- C. The script is run on the machine uploading the script to ensure that it is operational.
- D. The level of risk is assigned to the script upon import.

Answer: D

Explanation:
The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk determines the permissions and restrictions for running the script on endpoints. The levels of risk are:
Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.
The other options are incorrect for the following reasons:
A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.
C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. VB scripts are not supported by Cortex XDR, and will not run on the endpoints.
D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.
Reference:
Agent Script Library
Import a Script
Run Scripts on an Endpoint

NEW QUESTION # 74
......

- XDR-Analyst Pdf Demo Download □ XDR-Analyst Online Lab Simulation □ XDR-Analyst Pdf Demo Download □ Go to website { www.troytecdumps.com } open and search for 【 XDR-Analyst 】 to download for free □New XDR-Analyst Braindumps Ebook
- Real Palo Alto Networks XDR-Analyst Exam Question In PDF □ Open website 《 www.pdfvce.com 》 and search for ⇒ XDR-Analyst ⇐ for free download □Test XDR-Analyst Guide Online
- New XDR-Analyst Braindumps Sheet □ Test XDR-Analyst Guide Online □ XDR-Analyst Reliable Dumps Questions □ □ Open 【 www.examcollectionpass.com 】 enter ➡ XDR-Analyst □□□ and obtain a free download □XDR-Analyst Study Material
- Free PDF XDR-Analyst - Trustable Exam Palo Alto Networks XDR Analyst Outline □ Download ☀ XDR-Analyst □☀□ for free by simply entering ☀ www.pdfvce.com □☀□ website □XDR-Analyst Free Exam
- XDR-Analyst Reliable Dumps Questions □ New XDR-Analyst Braindumps Ebook □ XDR-Analyst Download Free Dumps □ Easily obtain free download of [XDR-Analyst] by searching on { www.dumpsmaterials.com } □Latest XDR-Analyst Exam Papers
- Latest XDR-Analyst Exam Materials: Palo Alto Networks XDR Analyst give you the most helpful Training Dumps □ Open 「 www.pdfvce.com 」 and search for ▹ XDR-Analyst ◃ to download exam materials for free □XDR-Analyst Dumps Guide
- Intereactive XDR-Analyst Testing Engine □ XDR-Analyst Dumps Guide □ XDR-Analyst Certification Book Torrent □ □ Search on ➠ www.testkingpass.com □ for { XDR-Analyst } to obtain exam materials for free download □XDR-Analyst Free Exam
- XDR-Analyst Exam Simulator Fee □ Practice XDR-Analyst Questions □ XDR-Analyst Reliable Dumps Questions □ Search for ➡ XDR-Analyst □□□ and download it for free on ➤ www.pdfvce.com □ website □XDR-Analyst Download Free Dumps
- Pass-Sure Exam XDR-Analyst Outline Offers Candidates Reliable Actual Palo Alto Networks Palo Alto Networks XDR Analyst Exam Products □ Enter ➤ www.practicevce.com □ and search for □ XDR-Analyst □ to download for free □ □New XDR-Analyst Braindumps Sheet
- Free PDF XDR-Analyst - Trustable Exam Palo Alto Networks XDR Analyst Outline □ Search for ➽ XDR-Analyst □ and download it for free on ➽ www.pdfvce.com □ website □Latest XDR-Analyst Braindumps Questions
- 100% Pass Authoritative XDR-Analyst - Exam Palo Alto Networks XDR Analyst Outline □ Search on [www.prep4sures.top] for ➠ XDR-Analyst □ to obtain exam materials for free download □XDR-Analyst Exam Sample Online
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.teachmenow.eu, www.stes.tyc.edu.tw, Disposable vapes