XDR-Analyst Actual Exam & XDR-Analyst Exam Guide & XDR-Analyst Practice Exam

Passing the XDR-Analyst certification can prove that you are very competent and excellent and you can also master useful knowledge and skill through passing the test. Purchasing our XDR-Analyst guide torrent can help you pass the exam and it costs little time and energy. The XDR-Analyst exam questions have simplified the sophisticated notions. The software boosts varied self-learning and self-assessment functions to check the learning results. The software of our XDR-Analyst Test Torrent provides the statistics report function and help the students find the weak links and deal with them.

These formats are Palo Alto Networks PDF Questions and practice test software. The Palo Alto Networks XDR Analyst XDR-Analyst practice exam software is further divided into two formats. The name of these two formats is Palo Alto Networks XDR-Analyst desktop practice test software and web-based Palo Alto Networks XDR-Analyst practice test software. Both Palo Alto Networks XDR-Analyst practice test software is the XDR-Analyst Practice Exam that will give you a real-time XDR-Analyst exam preparation environment to solve all Palo Alto Networks XDR Analyst XDR-Analyst questions. With the Palo Alto Networks XDR-Analyst practice test software you can understand your weak topic areas. Later on, working on these Palo Alto Networks XDR-Analyst weak topic areas you can make it perfect.

>> New XDR-Analyst Exam Notes <<

Instant Palo Alto Networks XDR-Analyst Discount & Frenquent XDR-Analyst Update

Our XDR-Analyst exam guide are not only rich and varied in test questions, but also of high quality. A very high hit rate gives you a good chance of passing the final XDR-Analyst exam. According to past statistics, 98 % - 99 % of the users who have used our XDR-Analyst Study Materials can pass the exam successfully. So without doubt, you will be our nest passer as well as long as you buy our XDR-Analystpractice braindumps.

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 (Q82-Q87):

NEW QUESTION # 82
Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

- A. role-based profiles that apply to specific endpoints
- B. exception profiles that apply to specific endpoints
- C. agent exception profiles that apply to specific endpoints
- D. global exception profiles that apply to all endpoints

Answer: C,D

Explanation:
Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. Reference:
Exception Security Profiles
Create an Agent Exception Profile
Create a Global Exception Profile

NEW QUESTION # 83
Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

- A. Cortex XDR Pro per Endpoint
- B. Cortex XDR Cloud per Host
- C. Cortex XDR Pro per TB
- D. Host Insights

Answer: B

Explanation:
When deploying Cortex XDR agent on Kubernetes clusters as a DaemonSet, the license required is Cortex XDR Cloud per Host. This license allows you to protect and monitor your cloud workloads, such as Kubernetes clusters, containers, and serverless functions, using Cortex XDR. With Cortex XDR Cloud per Host license, you can deploy Cortex XDR agents as DaemonSets on your Kubernetes clusters, which ensures that every node in the cluster runs a copy of the agent. The Cortex XDR agent collects and sends data from the Kubernetes cluster, such as pod events, container logs, and network traffic, to the Cortex Data Lake for analysis and correlation. Cortex XDR can then detect and respond to threats across your cloud environment, and provide visibility and context into your cloud workloads. The Cortex XDR Cloud per Host license is based on the number of hosts that run the Cortex XDR agent, regardless of the number of containers or functions on each host. A host is defined as a virtual machine, a

physical server, or a Kubernetes node that runs the Cortex XDR agent. You can read more about the Cortex XDR Cloud per Host license and how to deploy Cortex XDR agent on Kubernetes clusters here1 and here2. Reference:
Cortex XDR Cloud per Host License
Deploy Cortex XDR Agent on Kubernetes Clusters as a DaemonSet

NEW QUESTION # 84
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. Enable DLL Protection on all endpoints but there might be some false positives.
- B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- C. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.
- D. No step is required because the malicious document is already stopped.

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 # 85
What is by far the most common tactic used by ransomware to shut down a victim's operation?

- A. restricting access to administrative accounts to the victim
- B. preventing the victim from being able to access APIs to cripple infrastructure
- C. denying traffic out of the victims network until payment is received
- D. encrypting certain files to prevent access by the victim

Answer: D

Explanation:
Ransomware is a type of malicious software, or malware, that encrypts certain files or data on the victim's system or network and prevents them from accessing their data until they pay a ransom. This is by far the most common tactic used by ransomware to shut down a victim's operation, as it can cause costly disruptions, data loss, and reputational damage. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware can spread through various methods, such as phishing emails,

malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack1234 Reference:
What is Ransomware? | How to Protect Against Ransomware in 2023
Ransomware - Wikipedia
What is ransomware? | Ransomware meaning | Cloudflare
[What Is Ransomware? | Ransomware.org]
[Ransomware - FBI]

NEW QUESTION # 86
When is the wss (WebSocket Secure) protocol used?

- A. when the Cortex XDR agent establishes a bidirectional communication channel
- B. when the Cortex XDR agent downloads new security content
- C. when the Cortex XDR agent uploads alert data
- D. when the Cortex XDR agent connects to WildFire to upload files for analysis

Answer: A

Explanation:
The WSS (WebSocket Secure) protocol is an extension of the WebSocket protocol that provides a secure communication channel over the internet. It is used to establish a persistent, full-duplex communication channel between a client (in this case, the Cortex XDR agent) and a server (such as the Cortex XDR management console or other components). The Cortex XDR agent uses the WSS protocol to establish a secure and real-time bidirectional communication channel with the Cortex XDR management console or other components in the Palo Alto Networks security ecosystem. This communication channel allows the agent to send data, such as security events, alerts, and other relevant information, to the management console, and receive commands, policy updates, and responses in return. By using the WSS protocol, the Cortex XDR agent can maintain a persistent connection with the management console, which enables timely communication of security-related information and allows for efficient incident response and remediation actions. It's important to note that the other options mentioned in the question also involve communication between the Cortex XDR agent and various components, but they do not specifically mention the use of the WSS protocol. For example:
A . The Cortex XDR agent downloading new security content typically utilizes protocols like HTTP or HTTPS.
B . When the Cortex XDR agent uploads alert data, it may use protocols like HTTP or HTTPS to transmit the data securely.
C . When the Cortex XDR agent connects to WildFire to upload files for analysis, it typically uses protocols like HTTP or HTTPS.
Therefore, the correct answer is D, when the Cortex XDR agent establishes a bidirectional communication channel. Reference:
Device communication protocols - AWS IoT Core
WebSocket - Wikipedia
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) - Palo Alto Networks
[What are WebSockets? | Web Security Academy]
[Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification exam practice question and answer (Q&A) dump with detail explanation and reference available free, helpful to pass the Palo Alto Networks Certified Detection and Remediation Analyst PCDRA exam and earn Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification.]

NEW QUESTION # 87
......

- Reliable Study XDR-Analyst Questions □ New XDR-Analyst Real Test □ Latest XDR-Analyst Dumps Ebook □ Search for 《 XDR-Analyst 》 and download it for free immediately on [www.exam4labs.com] □Latest XDR-Analyst Exam Papers
- Reliable Study XDR-Analyst Questions □ Valuable XDR-Analyst Feedback □ New XDR-Analyst Exam Answers □ Download { XDR-Analyst } for free by simply entering □ www.pdfvce.com □ website □Latest XDR-Analyst Exam Papers
- 100% Pass Quiz XDR-Analyst - Palo Alto Networks XDR Analyst Pass-Sure New Exam Notes □ Easily obtain free download of □ XDR-Analyst □ by searching on ➥ www.examcollectionpass.com □ □Reliable Study XDR-Analyst Questions
- XDR-Analyst - Palo Alto Networks XDR Analyst –Professional New Exam Notes □ Download □ XDR-Analyst □ for free by simply entering " www.pdfvce.com " website □Latest XDR-Analyst Test Simulator
- Palo Alto Networks XDR-Analyst Guaranteed Success with Satisfied Customers and 24/7 Support System □ Download ✔ XDR-Analyst □✔□ for free by simply searching on 【 www.examcollectionpass.com 】 □XDR-Analyst New Practice Questions
- Palo Alto Networks XDR-Analyst Guaranteed Success with Satisfied Customers and 24/7 Support System □ Search for □ XDR-Analyst □ and download it for free immediately on ▷ www.pdfvce.com ◁ □Exam XDR-Analyst PDF
- Reasonable XDR-Analyst Exam Price □ Exam XDR-Analyst Certification Cost □ XDR-Analyst Reliable Dumps Book □ □ Search for ➡ XDR-Analyst □□□ on 【 www.testkingpass.com 】 immediately to obtain a free download □Exam XDR-Analyst PDF
- Exam XDR-Analyst PDF □ Exam XDR-Analyst PDF □ Reliable Study XDR-Analyst Questions □ Search for 《 XDR-Analyst 》 and obtain a free download on ➡ www.pdfvce.com □□□ □Key XDR-Analyst Concepts
- Diverse Formats for Palo Alto Networks XDR-Analyst Exam Questions: Choose What Works Best for You □ 《 www.exam4labs.com 》 is best website to obtain 《 XDR-Analyst 》 for free download □Training XDR-Analyst Material
- XDR-Analyst Reliable Dumps Book □ Latest XDR-Analyst Test Simulator □ Reasonable XDR-Analyst Exam Price □ □ Go to website ➡ www.pdfvce.com □□□ open and search for ➽ XDR-Analyst □ to download for free □Latest XDR-Analyst Dumps Ebook
- Latest XDR-Analyst Exam Papers □ Latest XDR-Analyst Dumps Ebook □ New XDR-Analyst Test Braindumps □ Open （ www.vce4dumps.com ） and search for ➠ XDR-Analyst □ to download exam materials for free □Latest XDR-Analyst Dumps Ebook
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, wjhsd.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes