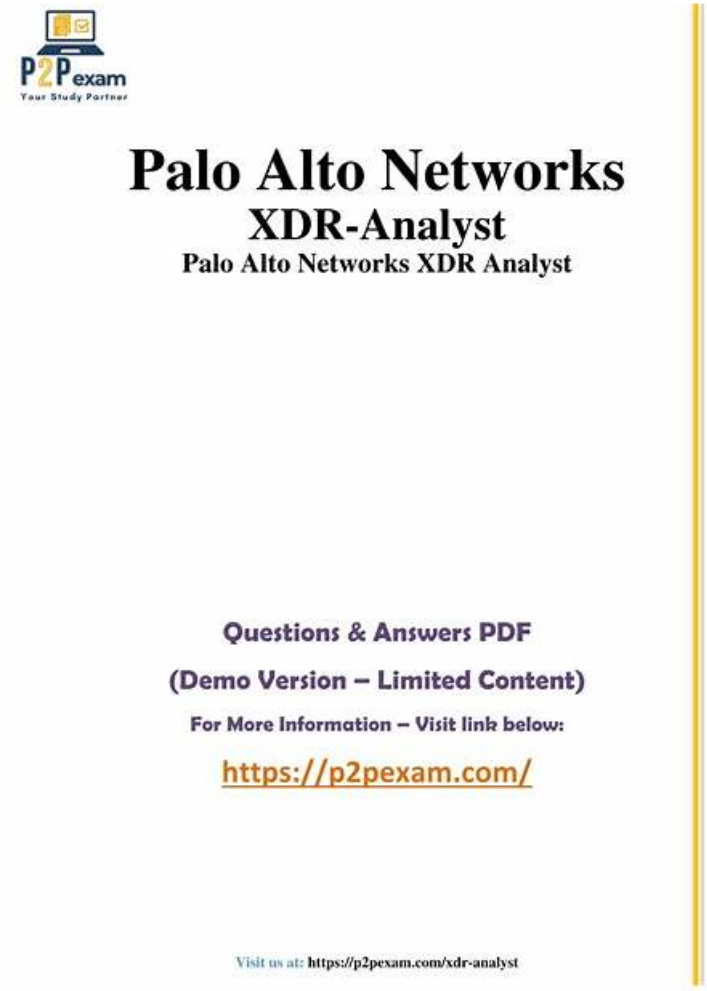
Palo Alto Networks XDR-Analyst PDF Questions-Turn Your Exam Fear Into Confidence



Valid Palo Alto Networks XDR Analyst XDR-Analyst test dumps demo and latest test preparation for customer's success. Palo Alto Networks offers latest Palo Alto Networks XDR Analyst exam and valid practice questions book to help you pass the Palo Alto Networks XDR Analyst XDR-Analyst Exam in your field. The Palo Alto Networks XDR Analyst exam is 365 days updates and true. New XDR-Analyst study questions pdf in less time. And Palo Alto Networks XDR Analyst XDR-Analyst price is benefit!

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	• 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	• 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.

>> Exam Dumps XDR-Analyst Free <<

XDR-Analyst Valid Braindumps Free - Valuable XDR-Analyst Feedback

Customers first are our mission, and we will try our best to help all of you to get your XDR-Analyst certification. We offer you the best valid and latest Palo Alto Networks XDR-Analyst study practice, thus you will save your time and study with clear direction. Besides, we provide you with best safety shopping experience. The Paypal system will guard your personal information and keep it secret. In addition, the high pass rate will ensure you pass your XDR-Analyst Certification with high score.

Palo Alto Networks XDR Analyst Sample Questions (Q70-Q75):

NEW QUESTION # 70
In the Cortex XDR console, from which two pages are you able to manually perform the agent upgrade action? (Choose two.)

- A. Action Center
- B. Asset Management
- C. Agent Installations
- D. Endpoint Administration

Answer: B,D

Explanation:
To manually upgrade the Cortex XDR agents, you can use the Asset Management page or the Endpoint Administration page in the Cortex XDR console. On the Asset Management page, you can select one or more endpoints and click Actions > Upgrade Agent. On the Endpoint Administration page, you can select one or more agent versions and click Upgrade. You can also schedule automatic agent upgrades using the Agent Installations page. Reference:
Asset Management
Endpoint Administration
Agent Installations

NEW QUESTION # 71
Why would one threaten to encrypt a hypervisor or, potentially, a multiple number of virtual machines running on a server?

- A. To better understand the underlying virtual infrastructure.
- B. To potentially perform a Distributed Denial of Attack.
- 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 # 72
Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

- A. Isolation
- B. Quarantine
- C. Flag for removal
- D. Search & destroy

Answer: B

Explanation:
The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. Reference:
Quarantine Files
Manage Quarantined Files

NEW QUESTION # 73
Where would you view the WildFire report in an incident?

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

Answer: B

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 # 74
Cortex XDR is deployed in the enterprise and you notice a cobalt strike attack via an ongoing supply chain compromise was prevented on 1 server. What steps can you take to ensure the same protection is extended to all your servers?

- A. Create IOCs of the malicious files you have found to prevent their execution.
- B. Enable DLL Protection on all servers but there might be some false positives.
- C. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
- D. Conduct a thorough Endpoint Malware scan.

Answer: A

Explanation:
The best step to ensure the same protection is extended to all your servers is to create indicators of compromise (IOCs) of the malicious files you have found to prevent their execution. IOCs are pieces of information that indicate a potential threat or compromise on an endpoint, such as file hashes, IP addresses, domain names, or registry keys. You can create IOCs in Cortex XDR to block or alert on any file or network activity that matches the IOCs. By creating IOCs of the malicious files involved in the cobalt strike attack, you can prevent them from running or spreading on any of your servers.
The other options are not the best steps for the following reasons:
A is not the best step because conducting a thorough Endpoint Malware scan may not detect or prevent the cobalt strike attack if the malicious files are obfuscated, encrypted, or hidden. Endpoint Malware scan is a feature of Cortex XDR that allows you to scan endpoints for known malware and quarantine any malicious files found. However, Endpoint Malware scan may not be effective against unknown or advanced threats that use evasion techniques to avoid detection.
B is not the best step because enabling DLL Protection on all servers may cause some false positives and disrupt legitimate applications. DLL Protection is a feature of Cortex XDR that allows you to block or alert on any DLL loading activity that matches certain criteria, such as unsigned DLLs, DLLs loaded from network locations, or DLLs loaded by specific processes. However, DLL Protection may also block or alert on benign DLL loading activity that is part of normal system or application operations, resulting in false positives and performance issues.
C is not the best step because enabling Behavioral Threat Protection (BTP) with cytool may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection. Behavioral Threat Protection is a feature of Cortex XDR that allows you to block or alert on any endpoint behavior that matches certain patterns, such as ransomware, credential theft, or lateral movement. Cytool is a command-line tool that allows you to configure and manage the Cortex XDR agent on the endpoint. However, Behavioral Threat Protection may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection, such as encryption, obfuscation, or proxy servers.
Reference:
Create IOCs
Scan an Endpoint for Malware
DLL Protection
Behavioral Threat Protection
Cytool for Windows

NEW QUESTION # 75
.....

www.pdfvce.com □□□ website □Latest XDR-Analyst Training

- Valid Exam XDR-Analyst Registration □ XDR-Analyst Reliable Braindumps Ebook □ XDR-Analyst Excellect Pass Rate □ Open ▹ www.exam4labs.com ◃ and search for ▸ XDR-Analyst ◂ to download exam materials for free □Test XDR-Analyst Free
- Exam Dumps XDR-Analyst Free | Efficient XDR-Analyst Valid Braindumps Free: Palo Alto Networks XDR Analyst □ Easily obtain free download of （ XDR-Analyst ） by searching on □ www.pdfvce.com □ □XDR-Analyst Reliable Braindumps Ebook
- High Pass-Rate Exam Dumps XDR-Analyst Free | Latest XDR-Analyst Valid Braindumps Free and Authorized Valuable Palo Alto Networks XDR Analyst Feedback □ Search on ➤ www.pass4test.com □ for ➠ XDR-Analyst □ to obtain exam materials for free download □Pdf XDR-Analyst Files
- Palo Alto Networks XDR-Analyst Questions - Exam Success Tips And Tricks □ Download { XDR-Analyst } for free by simply searching on □ www.pdfvce.com □ □XDR-Analyst Exam Overviews
- XDR-Analyst Practice Online □ XDR-Analyst Reliable Braindumps Ebook □ XDR-Analyst Excellect Pass Rate □ Open ▸ www.examcollectionpass.com ◂ and search for " XDR-Analyst " to download exam materials for free □XDR-Analyst Training Material
- XDR-Analyst Reliable Exam Pattern □ Latest XDR-Analyst Training □ XDR-Analyst Latest Test Simulations □ Search for □ XDR-Analyst □ and download it for free on ✔ www.pdfvce.com □✔□ website □XDR-Analyst Excellect Pass Rate
- Palo Alto Networks XDR Analyst Practice Vce - XDR-Analyst Training Material - Palo Alto Networks XDR Analyst Study Guide □ Easily obtain free download of ➠ XDR-Analyst □ by searching on ➥ www.vce4dumps.com □ □Test XDR-Analyst Free
- XDR-Analyst Reliable Exam Pattern □ XDR-Analyst Actual Test Pdf □ Pdf XDR-Analyst Files □ Download ✔ XDR-Analyst □✔□ for free by simply entering " www.pdfvce.com " website □XDR-Analyst PDF Question
- Latest Upload Exam Dumps XDR-Analyst Free - Palo Alto Networks Palo Alto Networks XDR Analyst Valid Braindumps Free □ Search for ➠ XDR-Analyst □ on ☀ www.pdfdumps.com □☀□ immediately to obtain a free download □ □XDR-Analyst Latest Test Simulations
-