Quiz Palo Alto Networks - XDR-Analyst - Palo Alto Networks XDR Analyst Perfect Dumps Discount

P.S. Free & New XDR-Analyst dumps are available on Google Drive shared by PDF4Test: https://drive.google.com/open?id=1MnXxe4dZ3mC2FQ2OdGFXcLWgzgQXItKX

We are benefiting more and more candidates for our excellent XDR-Analyst exam materials which is compiled by the professional experts accurately and skillfully. We are called the best friend on the way with our customers to help pass their XDR-Analyst exam and help achieve their dreaming certification. The reason is that we not only provide our customers with valid and reliable XDR-Analyst study questions, but also offer best service online since we uphold the professional ethical.

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.

>> Dumps XDR-Analyst Discount <<

XDR-Analyst Exam Tutorials & Exam XDR-Analyst Course

PDF version of XDR-Analyst exam questions - being legible to read and remember, support customers' printing request, and allow you to have a print and practice in papers. Software version of XDR-Analyst guide dump - supporting simulation test system, with times of setup has no restriction. Remember this version support Windows system users only. App online version of XDR-Analyst Guide dump -Being suitable to all kinds of equipment or digital devices, supportive to offline exercises on the condition that you practice it without mobile data. Bogged down in review process right now, our XDR-Analyst training materials with three versions can help you gain massive knowledge.

Palo Alto Networks XDR Analyst Sample Questions (Q77-Q82):

NEW QUESTION # 77
What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

- A. Worm
- B. Rootkit
- C. Keylogger
- D. Ransomware

Answer: D

Explanation:
The kind of malware that uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim is ransomware. Ransomware is a type of malware that encrypts the victim's files or blocks access to their system, and then demands a ransom for the decryption key or the restoration of access. Ransomware can also threaten to expose or delete the victim's data if the ransom is not paid. Ransomware can cause significant damage and disruption to individuals, businesses, and organizations, and can be difficult to remove or recover from. Some examples of ransomware are CryptoLocker, WannaCry, Ryuk, and REvil.
Reference:
12 Types of Malware + Examples That You Should Know - CrowdStrike
What is Malware? Malware Definition, Types and Protection
12+ Types of Malware Explained with Examples (Complete List)

NEW QUESTION # 78
What kind of the threat typically encrypts user files?

- A. supply-chain attacks
- B. ransomware
- C. SQL injection attacks
- D. Zero-day exploits

Answer: B

Explanation:
Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. 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 attack123456 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 # 79
When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

- A. The prevention archive from the alert.
- B. The unique agent id.
- C. A list of all the current exceptions applied to the agent.
- D. The distribution id of the agent.
- E. The agent technical support file.

Answer: A,E

Explanation:
When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:
The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.
The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.
The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:
The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.
A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.
The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.
Reference:
Generate and Download the Agent Technical Support File
Generate and Download the Prevention Archive
Cortex XDR Agent Administrator Guide: Agent Distribution ID
Cortex XDR Agent Administrator Guide: Exception Security Profiles
[Cortex XDR Agent Administrator Guide: Unique Agent ID]

NEW QUESTION # 80
What is an example of an attack vector for ransomware?

- A. A URL filtering feature enabled on a firewall
- B. Performing SSL Decryption on an endpoint
- C. Performing DNS queries for suspicious domains
- D. Phishing emails containing malicious attachments

Answer: D

Explanation:
An example of an attack vector for ransomware is phishing emails containing malicious attachments. Phishing is a technique that involves sending fraudulent emails that appear to come from a legitimate source, such as a bank, a company, or a government agency. The emails typically contain a malicious attachment, such as a PDF document, a ZIP archive, or a Microsoft Office document, that contains ransomware or a ransomware downloader. When the recipient opens or downloads the attachment, the ransomware is executed and encrypts the files or data on the victim's system. The attacker then demands a ransom for the decryption key, usually in cryptocurrency.
Phishing emails are one of the most common and effective ways of delivering ransomware, as they can bypass security measures such as firewalls, antivirus software, or URL filtering. Phishing emails can also exploit the human factor, as they can trick the recipient into opening the attachment by using social engineering techniques, such as impersonating a trusted sender, creating a sense of urgency, or appealing to curiosity or greed. Phishing emails can also target specific individuals or organizations, such as executives, employees, or customers, in a technique called spear phishing, which increases the chances of success.
According to various sources, phishing emails are the main vector of ransomware attacks, accounting for more than 90% of all ransomware infections12. Some of the most notorious ransomware campaigns, such as CryptoLocker, Locky, and WannaCry, have used phishing emails as their primary delivery method3 . Therefore, it is essential to educate users on how to recognize and avoid phishing emails, as well as to implement security solutions that can detect and block malicious attachments. Reference:
Top 7 Ransomware Attack Vectors & How to Avoid Becoming a Victim - Bitsight What Is the Main Vector of Ransomware Attacks? A Definitive Guide CryptoLocker Ransomware Information Guide and FAQ
[Locky Ransomware Information, Help Guide, and FAQ]

[WannaCry ransomware attack]

NEW QUESTION # 81
Which Type of IOC can you define in Cortex XDR?

- A. App-ID
- B. full path
- C. e-mail address
- D. destination port

Answer: B

Explanation:
Cortex XDR allows you to define IOCs based on various criteria, such as file hashes, registry keys, IP addresses, domain names, and full paths. A full path IOC is a specific location of a file or folder on an endpoint, such as C:\Windows\System32\calc.exe. You can use full path IOCs to detect and respond to malicious files or folders that are located in known locations on your endpoints12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . destination port: This is not the correct answer. Destination port is not a type of IOC that you can define in Cortex XDR. Destination port is a network attribute that indicates the port number to which a packet is sent. Cortex XDR does not support defining IOCs based on destination ports, but you can use XQL queries to filter network events by destination ports3.
B . e-mail address: This is not the correct answer. E-mail address is not a type of IOC that you can define in Cortex XDR. E-mail address is an identifier that is used to send and receive e-mails. Cortex XDR does not support defining IOCs based on e-mail addresses, but you can use the Cortex XDR - IOC integration with Cortex XSOAR to ingest IOCs from various sources, including e-mail addresses4.
D . App-ID: This is not the correct answer. App-ID is not a type of IOC that you can define in Cortex XDR. App-ID is a feature of Palo Alto Networks firewalls that identifies and controls applications on the network. Cortex XDR does not support defining IOCs based on App-IDs, but you can use the Cortex XDR Analytics app to create custom rules that use App-IDs as part of the rule logic5.
In conclusion, full path is the type of IOC that you can define in Cortex XDR. By using full path IOCs, you can enhance your detection and response capabilities and protect your endpoints from malicious files or folders.
Reference:
Create an IOC Rule
XQL Reference Guide: Network Events Schema
Cortex XDR - IOC
Cortex XDR Analytics App
PCDRA: Which Type of IOC can define in Cortex XDR?

NEW QUESTION # 82
.....

We offer a money-back guarantee, which means we are obliged to return 100% of your sum (terms and conditions apply) in case of any unsatisfactory results. Even though the Palo Alto Networks experts who have designed XDR-Analyst assure us that anyone who studies properly cannot fail the exam, we still offer a money-back guarantee. This way we prevent pre and post-purchase anxiety.

www.troytecdumps.com ◁ open and search for ⇛ XDR-Analyst ⇚ to download for free □XDR-Analyst Latest Exam Forum

- Palo Alto Networks - Authoritative Dumps XDR-Analyst Discount □ Download □ XDR-Analyst □ for free by simply entering （ www.pdfvce.com ） website □XDR-Analyst Dumps Free Download
- XDR-Analyst Relevant Exam Dumps □ Test XDR-Analyst Engine Version □ XDR-Analyst Latest Exam Forum □ Search for ➤ XDR-Analyst □ and download it for free on 《 www.pass4test.com 》 website □XDR-Analyst Valid Practice Materials
- XDR-Analyst Latest Braindumps Ppt □ XDR-Analyst Latest Braindumps Ppt □ Valid Exam XDR-Analyst Preparation □ ➥ www.pdfvce.com □ is best website to obtain ⇛ XDR-Analyst ⇚ for free download □XDR-Analyst Actual Test Answers
- XDR-Analyst Reliable Exam Tips □ Valid Exam XDR-Analyst Preparation □ XDR-Analyst Latest Exam Pdf □ Download [XDR-Analyst] for free by simply searching on ▶ www.verifieddumps.com ◀ □XDR-Analyst Valid Exam Labs
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, 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, bbs.t-firefly.com, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of PDF4Test XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1MnXxe4dZ3mC2FQ2OdGFXcLWgzgQXItKX