PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pcdra.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

Correct Answer: C

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. References: 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?

QUESTION 2

What motivation do ransomware attackers have for returning access to systems once their victims have paid?

A. There is organized crime governance among attackers that requires the return of access to remain in good standing.
B. Nation-states enforce the return of system access through the use of laws and regulation.

B. Failure to restore access to systems undermines the scheme because others will not believe their valuables would be returned.

C. The ransomware attackers hope to trace the financial trail back and steal more from traditional banking institutions.

Correct Answer: C

Explanation: Ransomware attackers have a motivation to return access to systems once their victims have paid

because they want to maintain their reputation and credibility. If they fail to restore access to systems, they risk losing the trust of future victims who may not believe that paying the ransom will result in getting their data back. This would reduce the effectiveness and profitability of their scheme. Therefore, ransomware attackers have an incentive to honor their promises and decrypt the data after receiving the ransom. References: What is the motivation behind ransomware? | Foresite As Ransomware Attackers\\' Motives Change, So Should Your Defense - Forbes

QUESTION 3

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Correct Answer: AB

Explanation: When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 References: Assign Incidents to an Analyst in Bulk Change the Status of Multiple Incidents

QUESTION 4

Where would you view the WildFire report in an incident?

A. next to relevant Key Artifacts in the incidents details page

B. under Response --> Action Center

C. under the gear icon --> Agent Audit Logs

D. on the HUB page at apps.paloaltonetworks.com

Correct Answer: A

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. References: View Incident Details View WildFire Reports Action Center Agent Audit Logs HUB

QUESTION 5

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

A. preventing the victim from being able to access APIs to cripple infrastructure

B. denying traffic out of the victims network until payment is received

C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Correct 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 References: 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]