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.geekcert.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the purpose of the Cortex Data Lake?

A. a local storage facility where your logs and alert data can be aggregated

B. a cloud-based storage facility where your firewall logs are stored

C. the interface between firewalls and the Cortex XDR agents

D. the workspace for your Cortex XDR agents to detonate potential malware files

Correct Answer: B

Explanation: The purpose of the Cortex Data Lake is to provide a cloud-based storage facility where your firewall logs are stored. Cortex Data Lake is a service that collects, transforms, and integrates your enterprise\\'s security data to enable Palo Alto Networks solutions. It powers AI and machine learning, detection accuracy, and app and service innovation. Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure, including your next-generation firewalls, Prisma Access, and Cortex XDR. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is available in multiple regions and supports data residency and privacy requirements. References: Cortex Data Lake - Palo Alto Networks Cortex Data Lake - Palo Alto Networks Cortex Data Lake, the technology behind Cortex XDR - Palo Alto Networks CORTEX DATA LAKE - Palo Alto Networks Sizing for Cortex Data Lake Storage - Palo Alto Networks

QUESTION 2

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 3

Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP

B. WebSocket

C. UDP and a random port

D. TCP, over port 80

Correct Answer: B

Explanation: Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. References: Initiate a Live Terminal Session WebSocket

QUESTION 4

What is an example of an attack vector for ransomware?

A. Performing DNS queries for suspicious domains

B. Performing SSL Decryption on an endpoint

C. Phishing emails containing malicious attachments

D. A URL filtering feature enabled on a firewall

Correct Answer: C

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 alegitimate 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. References: Top 7 Ransomware Attack Vectors and 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]

QUESTION 5

What is the difference between presets and datasets in XQL?

A. A dataset is a Cortex data lake data source only; presets are built-in data source.

B. A dataset is a built-in orthird-partysource; presets group XDR data fields.

C. A dataset is a database; presets is a field.

D. A dataset is a third-party data source; presets are built-in data source.

Correct Answer: B

Explanation: The difference between presets and datasets in XQL is that a dataset is a built-in or third-party data source, while a preset is a group of XDR data fields. A dataset is a collection of data that you can query and analyze using XQL.

A dataset can be a Cortex data lake data source, such as endpoints, alerts, incidents, or network flows, or a third- party data source, such as AWS CloudTrail, Azure Activity Logs, or Google Cloud Audit Logs. A preset is a predefined set of

XDR data fields that are relevant for a specific use case, such as process execution, file operations, or network activity. A preset can help you simplify and standardize your XQL queries by selecting the most important fields for youranalysis.

You can use presets with any Cortex data lake data source, but not with third-party data sources. References:

Datasets and Presets

XQL Language Reference