



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

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



**QUESTION 1**

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically close the connections involved in malicious traffic.
- B. Automatically kill the processes involved in malicious activity.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically block the IP addresses involved in malicious traffic.

Correct Answer: BD

Explanation: The "Respond to Malicious Causality Chains" feature in a Cortex XDR Windows Malware profile allows the agent to take automatic actions against network connections and processes that are involved in malicious activity on the

endpoint. The feature has two modes: Block IP Address and Kill Process1. The two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile are:

Automatically kill the processes involved in malicious activity. This can help to stop the malware from spreading or doing any further damage. Automatically block the IP addresses involved in malicious traffic. This can help to prevent the

malware from communicating with its command and control server or other malicious hosts.

The other two options, automatically close the connections involved in malicious traffic and automatically terminate the threads involved in malicious activity, are not specific to "Respond to Malicious Causality Chains". They are general

security measures that the agent can perform regardless of the feature.

References:

Cortex XDR Agent Security Profiles

Cortex XDR Agent 7.5 Release Notes

PCDRA: What are purposes of "Respond to Malicious Causality Chains" in ...

QUESTION 2

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

- A. Broker VM Pathfinder
- B. Local Agent Proxy
- C. Local Agent Installer and Content Caching
- D. Broker VM Syslog Collector

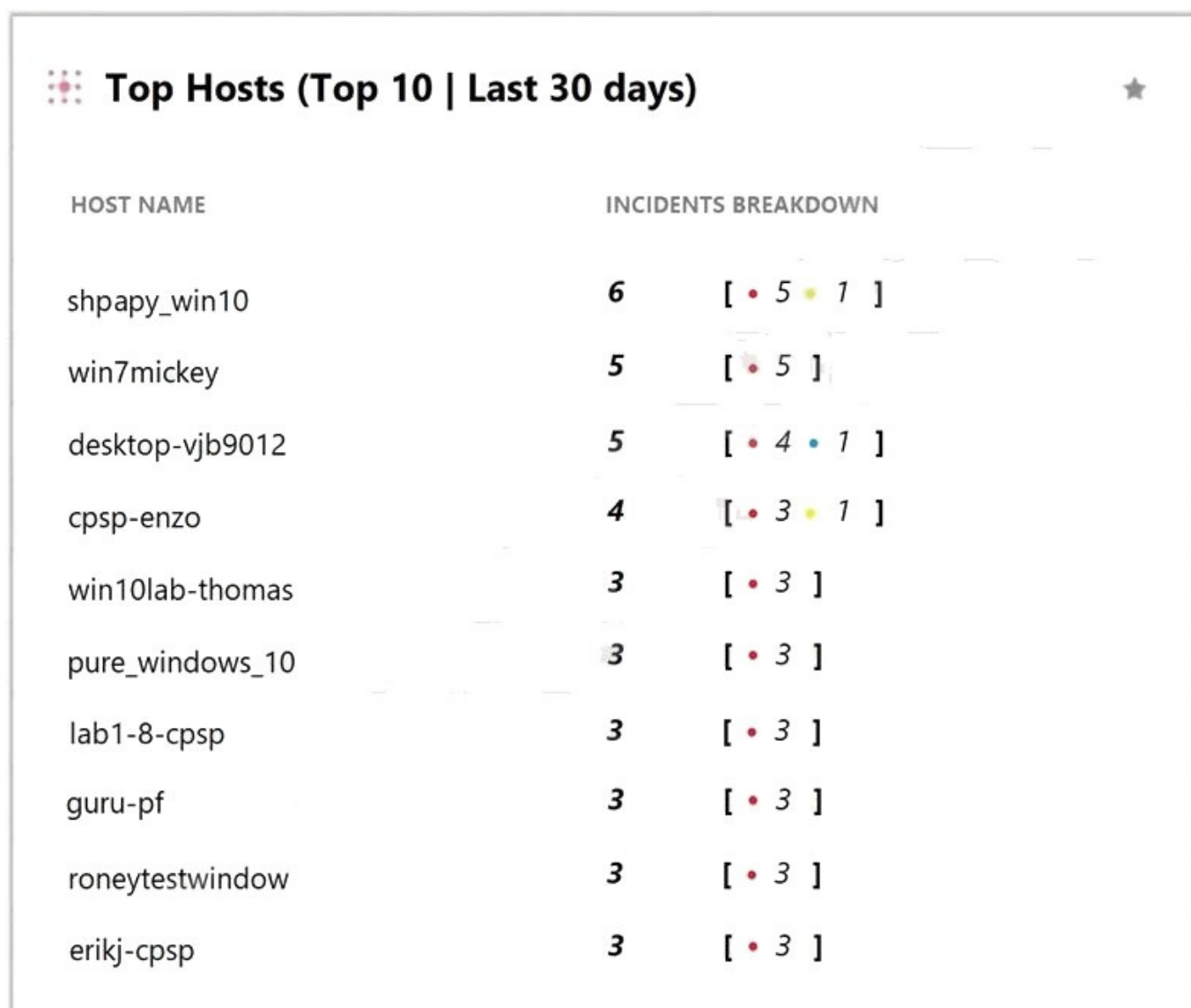


Correct Answer: B

Explanation: If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it here¹ and here². References: Local Agent Proxy Configure the Local Agent Proxy Setup

QUESTION 3

What does the following output tell us?





- A. There is one low severity incident.
- B. Host shpapy_win10 had the most vulnerabilities.
- C. There is one informational severity alert.
- D. This is an actual output of the Top 10 hosts with the most malware.

Correct Answer: D

Explanation: The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more . References: Use the ACC to Analyze Network Activity Top 10 Hosts with the Most Malware

QUESTION 4

In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

- A. Create a custom XQL widget
- B. This is not currently supported
- C. Create a custom report and filter on starred incidents
- D. Click the star in the widget

Correct Answer: D

Explanation: To filter the display to only show incidents that were "starred", you need to click the star in the widget. This will apply a filter that shows only the incidents that contain a starred alert, which is an alert that matches a specific condition that you define in the incident starring configuration. You can use the incident starring feature to prioritize and focus on the most important or relevant incidents in your environment¹. Let's briefly discuss the other options to provide a comprehensive explanation:

A. Create a custom XQL widget: This is not the correct answer. Creating a custom XQL widget is not necessary to filter the display to only show starred incidents. A custom XQL widget is a widget that you create by using the XQL query language to define the data source and the visualization type. You can use custom XQL widgets to create your own dashboards or reports, but they are not required for filtering incidents by stars². B. This is not currently supported: This is not the correct answer. Filtering the display to only show starred incidents is currently supported by Cortex XDR. You can use the star icon in the widget to apply this filter, or you can use the Filter Builder to create a custom filter based on the Starred field¹.

C. Create a custom report and filter on starred incidents: This is not the correct answer. Creating a custom report and filtering on starred incidents is not the only way to filter the display to only show starred incidents. A custom report is a report that you create by using the Report Builder to define the data source, the layout, and the schedule. You can use custom reports to generate and share periodic reports on your Cortex XDR data, but they are not the only option for filtering incidents by stars³. In conclusion, clicking the star in the widget is the simplest and easiest way to filter the display to only show incidents that were "starred". By using this feature, you can quickly identify and focus on the most critical or relevant incidents in your environment. References: Filter Incidents by Stars Create a Custom XQL Widget Create a Custom Report

**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]

[PCDRA PDF Dumps](#)

[PCDRA Practice Test](#)

[PCDRA Study Guide](#)