



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

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. Conduct a thorough Endpoint Malware scan.
- 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. Create IOCs of the malicious files you have found to prevent their execution.



Correct Answer: D

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. References: Create IOCs Scan an Endpoint for Malware DLL Protection Behavioral Threat Protection Cytool for Windows

QUESTION 3

What is the function of WildFire for Cortex XDR?

- A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.
- B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.
- C. WildFire accepts and analyses a sample to provide a verdict.
- D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Correct Answer: C

Explanation: WildFire is a cloud-based service that accepts and analyses samples from various sources, including Cortex XDR, to provide a verdict of malware, benign, or grayware. WildFire also generates detailed analysis reports that show the behaviour and characteristics of the samples. Cortex XDR uses WildFire verdicts and reports to enhance its detection and prevention capabilities, as well as to provide more visibility and context into the threats. References: WildFire Analysis Concepts WildFire Overview

QUESTION 4

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

- A. by encrypting the disk first.



- B. by utilizing decoy Files.
- C. by retrieving the encryption key.
- D. by patching vulnerable applications.

Correct Answer: B

Explanation: Cortex XDR agent for Windows prevents ransomware attacks from compromising the file system by utilizing decoy files. Decoy files are randomly generated files that are placed in strategic locations on the endpoint, such as the user's desktop, documents, and pictures folders. These files are designed to look like valuable data that ransomware would target for encryption. When Cortex XDR agent detects that a process is attempting to access or modify a decoy file, it immediately blocks the process and alerts the administrator. This way, Cortex XDR agent can stop ransomware attacks before they can cause any damage to the real files on the endpoint. References: Anti-Ransomware Protection PCDRA Study Guide

QUESTION 5

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

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

Correct Answer: A

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.

References:

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)

[Latest PCDRA Dumps](#)

[PCDRA PDF Dumps](#)

[PCDRA Study Guide](#)