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.passapply.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

With a Cortex XDR Prevent license, which objects are considered to be sensors?

A. Syslog servers

B. Third-Party security devices

C. Cortex XDR agents

D. Palo Alto Networks Next-Generation Firewalls

Correct Answer: C

Explanation: The objects that are considered to be sensors with a Cortex XDR Prevent license are Cortex XDR agents and Palo Alto Networks Next-Generation Firewalls. These are the two sources of data that Cortex XDR can collect and analyze for threat detection and response. Cortex XDR agents are software components that run on endpoints, such as Windows, Linux, and Mac devices, and provide protection against malware, exploits, and fileless attacks. Cortex XDR agents also collect and send endpoint data, such as process activity, network traffic, registry changes, and user actions, to the Cortex Data Lake for analysis and correlation. Palo Alto Networks Next-Generation Firewalls are network security devices that provide visibility and control over network traffic, and enforce security policies based on applications, users, and content. Next-Generation Firewalls also collect and send network data, such as firewall logs, DNS logs, HTTP headers, and WildFire verdicts, to the Cortex Data Lake for analysis and correlation. By integrating data from both Cortex XDR agents and Next-Generation Firewalls, Cortex XDR can provide a comprehensive view of the attack surface and detect threats across the network and endpoint layers. References: Cortex XDR Prevent License Cortex XDR Agent Features Next-Generation Firewall Features

QUESTION 2

Which type of IOC can you define in Cortex XDR?

A. Destination IP Address

B. Source IP Address

C. Source port

D. Destination IPAddress: Destination

Correct Answer: A

Explanation: Cortex XDR allows you to define IOC rules based on various types of indicators of compromise (IOC) that you can use to detect and respond to threats in your network. One of the types of IOC that you can define in Cortex XDR is destination IP address, which is the IP address of the remote host that a local endpoint is communicating with. You can use this type of IOC to identify malicious network activity, such as connections to command and control servers, phishing sites, or malware distribution hosts. You can also specify the direction of the network traffic (inbound or outbound) and the protocol (TCP or UDP) for the destination IP address IOC. References: Cortex XDR documentation portal Is there a possibility to create an IOC list to employ it in a query? Cortex XDR Datasheet

QUESTION 3

What is the Wildfire analysis file size limit for Windows PE files?

A. No Limit

B. 500MB

C. 100MB

D. 1GB

Correct Answer: C

Explanation: The Wildfire analysis file size limit for Windows PE files is 100MB. Windows PE files are executable files that run on the Windows operating system, such as .exe, .dll, .sys, or .scr files. Wildfire is a cloud-based service that analyzes files and URLs for malicious behavior and generates signatures and protections for them. Wildfire can analyze various file types, such as PE, APK, PDF, MS Office, and others, but each file type has a different file size limit. The file size limit determines the maximum size of the file that can be uploaded or forwarded to Wildfire for analysis. If the file size exceeds the limit, Wildfire will not analyze the file and will return an error message. According to the Wildfire documentation1, the file size limit for Windows PE files is 100MB. This means that any PE file that is larger than 100MB will not be analyzed by Wildfire. However, the firewall can still apply other security features, such as antivirus, antispyware, vulnerability protection, and file blocking, to the PE file based on the security policy settings. The firewall can also perform local analysis on the PE file using the Cortex XDR agent, which uses machine learning models to assess the file and assign it a verdict2. References: WildFire File Size Limits: This document provides the file size limits for different file types that can be analyzed by Wildfire. Local Analysis: This document explains how the Cortex XDR agent performs local analysis on files that cannot be sent to Wildfire for analysis.

QUESTION 4

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

A. Cortex XDR Pro per TB

B. Host Insights

C. Cortex XDR Pro per Endpoint

D. Cortex XDR Cloud per Host

Correct Answer: D

Explanation: When deploying Cortex XDR agent on Kubernetes clusters as a DaemonSet, the license required is Cortex XDR Cloud per Host. This license allows you to protect and monitor your cloud workloads, such as Kubernetes clusters, containers, and serverless functions, using Cortex XDR. With Cortex XDR Cloud per Host license, you can deploy Cortex XDR agents as DaemonSets on your Kubernetes clusters, which ensures that every node in the cluster runs a copy of the agent. The Cortex XDR agent collects and sends data from the Kubernetes cluster, such as pod events, container logs, and network traffic, to the Cortex Data Lake for analysis and correlation. Cortex XDR can then detect and respond to threats across your cloud environment, and provide visibility and context into your cloud workloads. The Cortex XDR Cloud per Host license is based on the number of hosts that run the Cortex XDR agent, regardless of the number of containers or functions on each host. A host is defined as a virtual machine, a physical server, or a Kubernetes node that runs the Cortex XDR agent. You can read more about the Cortex XDR Cloud per Host license and how to deploy Cortex XDR agent on Kubernetes clusters here1 and here2. References: Cortex XDR Cloud per Host License Deploy Cortex XDR Agent on Kubernetes Clusters as a DaemonSet

QUESTION 5

Which of the following is NOT a precanned script provided by Palo Alto Networks?

A. delete_file

B. quarantine_file

C. process_kill_name

D. list_directories

Correct Answer: D

Explanation: Palo Alto Networks provides a set of precanned scripts that you can use to perform various actions on your endpoints, such as deleting files, killing processes, or quarantining malware. The precanned scripts are written in Python

and are available in the Agent Script Library in the Cortex XDR console. You can use the precanned scripts as they are, or you can customize them to suit your needs. The precanned scripts are:

delete_file: Deletes a specific file from a local or removable drive. quarantine_file: Moves a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed. process_kill_name: Kills a

process by its name on the endpoint. process_kill_pid: Kills a process by its process ID (PID) on the endpoint. process_kill_tree: Kills a process and all its child processes by its name on the endpoint.

process_kill_tree_pid: Kills a process and all its child processes by its PID on the endpoint.

process_list: Lists all the processes running on the endpoint, along with their names, PIDs, and command lines.

process_list_tree: Lists all the processes running on the endpoint, along with their names, PIDs, command lines, and parent processes.

process_start: Starts a process on the endpoint by its name or path. registry_delete_key: Deletes a registry key and all its subkeys and values from the Windows registry.

registry_delete_value: Deletes a registry value from the Windows registry. registry_list_key: Lists all the subkeys and values under a registry key in the Windows registry.

registry_list_value: Lists the value and data of a registry value in the Windows registry.

registry_set_value: Sets the value and data of a registry value in the Windows registry.

The script list_directories is not a precanned script provided by Palo Alto Networks. It is a custom script that you can write yourself using Python commands.

References:

Run Scripts on an Endpoint

Agent Script Library

Precanned Scripts

Latest PCDRA Dumps PCDRA VCE Dumps PCDRA Exam Questions