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

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

A. causality_chain

B. endpoint_name

C. threat_event

D. event_type

Correct Answer: D

Explanation: To create a BIOC rule with XQL query, you must at a minimum filter on the event_type field in order for it to be a valid BIOC rule. The event_type field indicates the type of event that triggered the alert, such as PROCESS, FILE, REGISTRY, NETWORK, or USER_ACCOUNT. Filtering on this field helps you narrow down the scope of your query and focus on the relevant events for your use case. Other fields, such as causality_chain, endpoint_name, threat_event, are optional and can be used to further refine your query or display additional information in the alert. References: Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, BIOC Rule Query Syntax

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 maximum number of agents one Broker VM local agent applet can support?

A. 5,000

B. 10,000

C. 15,000

D. 20,000

Correct Answer: B

Explanation: The Broker VM is a virtual machine that you can deploy in your network to provide various services and functionalities to the Cortex XDR agents. One of the services that the Broker VM offers is the Local Agent Settings applet,

which allows you to configure the agent proxy, agent installer, and content caching settings for the agents. The Local Agent Settings applet can support a maximum number of 10,000 agents per Broker VM. If you have more than 10,000

agents in your network, you need to deploy additional Broker VMs and distribute the load among them. References:

Broker VM Overview: This document provides an overview of the Broker VM and its features, requirements, and deployment options. Configure the Broker VM: This document explains how to install, set up, and configure the Broker VM in an

ESXi environment.

Manage Broker VM from the Cortex XDR Management Console: This document describes how to activate and manage the Broker VM applets from the Cortex XDR management console.

QUESTION 4

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 lOCs 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 5

You can star security events in which two ways? (Choose two.)

A. Create an alert-starring configuration.

B. Create an Incident-starring configuration.

C. Manually star an alert.

D. Manually star an Incident.

Correct Answer: CD

Explanation: You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you prioritize and track the events that are most important to you. You can also filter and sort the events by their star status in the Cortex XDR console. To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again. To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed. References: Star Security Events Create an Alert Starring Configuration Create an Incident Starring Configuration