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

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

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

QUESTION 3

Which statement is true for Application Exploits and Kernel Exploits?

A. The ultimate goal of any exploit is to reach the application.

B. Kernel exploits are easier to prevent then application exploits.

C. The ultimate goal of any exploit is to reach the kernel.

D. Application exploits leverage kernel vulnerability.

Correct Answer: C

Explanation: The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than application exploits, because they can bypass security mechanisms and hide their presence from the user and the system. References: Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

QUESTION 4

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

Explanation: Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities12. Let\\'s briefly discuss the other options to provide a comprehensive explanation:

A. Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents3. B. Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server4.

C. Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints5. In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture

and protect against the latest cyberthreats. References: About Unit 42: Our Mission and Team Unit 42: Threat Intelligence and Response Cortex XSOAR Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

QUESTION 5

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.