Free Questions for PCDRA by certscare

Shared by Sellers on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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

Options:

A- Cortex XDR Pro per TB

B- Host Insights

C- Cortex XDR Pro per Endpoint

D- Cortex XDR Cloud per Host

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 here1and here2.Reference:

Cortex XDR Cloud per Host License

Deploy Cortex XDR Agent on Kubernetes Clusters as a DaemonSet

Question 2

Question Type: **MultipleChoice**

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

Options:

A- Syslog servers

B- Third-Party security devices

C- Cortex XDR agents

D- Palo Alto Networks Next-Generation Firewalls

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.Reference:

Cortex XDR Prevent License

Cortex XDR Agent Features

Next-Generation Firewall Features

Question 3

Question Type: **MultipleChoice**

When is the wss (WebSocket Secure) protocol used?

Options:

A- when the Cortex XDR agent downloads new security content

B- when the Cortex XDR agent uploads alert data

C- when the Cortex XDR agent connects to WildFire to upload files for analysis

D- when the Cortex XDR agent establishes a bidirectional communication channel

Answer:

D

Explanation:

The WSS (WebSocket Secure) protocol is an extension of the WebSocket protocol that provides a secure communication channel over the internet. It is used to establish a persistent, full-duplex communication channel between a client (in this case, the Cortex XDR agent) and a server (such as the Cortex XDR management console or other components). The Cortex XDR agent uses the WSS protocol to establish a secure and real-time bidirectional communication channel with the Cortex XDR management console or other components in the Palo Alto Networks security ecosystem. This communication channel allows the agent to send data, such as security events, alerts, and other relevant information, to the management console, and receive commands, policy updates, and responses in return. By using the WSS protocol, the Cortex XDR agent can maintain a persistent connection with the management console, which enables timely communication of security-related information and allows for efficient incident response and remediation actions. It's important to note that the other options mentioned in the question also involve communication between the Cortex XDR agent and various components, but they do not specifically mention the use of the WSS protocol. For example:

A) The Cortex XDR agent downloading new security content typically utilizes protocols like HTTP or HTTPS.

B) When the Cortex XDR agent uploads alert data, it may use protocols like HTTP or HTTPS to transmit the data securely.

C) When the Cortex XDR agent connects to WildFire to upload files for analysis, it typically uses protocols like HTTP or HTTPS. Therefore, the correct answer is D, when the Cortex XDR agent establishes a bidirectional communication channel.Reference:

Device communication protocols -- AWS IoT Core

WebSocket -- Wikipedia

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) -- Palo Alto Networks

[What are WebSockets? | Web Security Academy]

[Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification exam practice question and answer (Q&A) dump with detail explanation and reference available free, helpful to pass the Palo Alto Networks Certified Detection and Remediation Analyst PCDRA exam and earn Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification.]

Question 4

Question Type: **MultipleChoice**

In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

Options:

A- Agent Proxy

B- Agent Installer and Content Caching

C- Syslog Collector

D- CSV Collector

Answer:

B

Explanation:

The Agent Installer and Content Caching applet of the Broker VM is used to download and cache the Cortex XDR agent installation packages and content updates from Palo Alto Networks servers. This applet also acts as a proxy server for the Cortex XDR agents to communicate with the Cortex Data Lake and the Cortex XDR management console. To ensure secure communication between the Broker VM and the Cortex XDR agents, you are required to install a strong cipher SHA256-based SSL certificate on the Broker VM. The SSL certificate must have a common name or subject alternative name that matches the Broker VM FQDN or IP address. The SSL certificate must also be trusted by the Cortex XDR agents, either by using a certificate signed by a public CA or by manually installing the certificate on the endpoints.Reference:

Agent Installer and Content Caching

Install an SSL Certificate on the Broker VM

Question 5

Question Type: MultipleChoice

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

Options:

A- Netflow Collector

B- Syslog Collector

C- DB Collector

D- Pathfinder

Answer:

B

Explanation:

The Broker VM is a virtual machine that acts as a data broker between third-party data sources and the Cortex Data Lake. It can ingest different types of data, such as syslog, netflow, database, and pathfinder. The Syslog Collector functionality of the Broker VM allows it to receive syslog messages from third-party devices, such as firewalls, routers, switches, and servers, and forward them to the Cortex Data Lake. The Syslog Collector can be configured to filter, parse, and enrich the syslog messages before sending them to the Cortex Data Lake. The Syslog Collector can also be used to ingest logs from third-party firewall vendors, such as Cisco, Fortinet, and Check Point, to the Cortex Data Lake. This enables Cortex XDR to analyze the firewall logs and provide visibility and threat detection across the network perimeter.Reference:

Cortex XDR Data Broker VM

Syslog Collector

Supported Third-Party Firewall Vendors

Question 6

Question Type: **MultipleChoice**

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

Options:

A- by encrypting the disk first.

B- by utilizing decoy Files.

C- by retrieving the encryption key.

D- by patching vulnerable applications.

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.Reference:

Anti-Ransomware Protection

PCDRA Study Guide

Question 7

Question Type: **MultipleChoice**

Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

Options:

A- in the macOS Malware Protection Profile to indicate allowed signers

B- in the Linux Malware Protection Profile to indicate allowed Java libraries

C- SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles

D- in the Windows Malware Protection Profile to indicate allowed executables

Answer:

D

Explanation:

Cortex XDR Malware Protection Profiles allow you to configure the malware prevention settings for Windows, Linux, and macOS endpoints. You can use SHA256 hash values in the Windows Malware Protection Profile to indicate allowed executables that you want to exclude from malware scanning. This can help you reduce false positives and improve performance by skipping the scanning of known benign files. You can add up to 1000 SHA256 hash values per profile. You cannot use SHA256 hash values in the Linux or macOS Malware Protection Profiles, but you can use other criteria such as file path, file name, or signer to exclude files from scanning.Reference:

Malware Protection Profiles

Configure a Windows Malware Protection Profile

PCDRA Study Guide

Question 8

Question Type: MultipleChoice

What is the standard installation disk space recommended to install a Broker VM?

Options:

A- 1GB disk space

B- 2GB disk space

C- 512GB disk space

D- 256GB disk space

Answer:

D

Explanation:

The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location. The system requirements for the Broker VM are as follows:

CPU: 4 cores

RAM: 8 GB

Disk space: 256 GB

Network: Internet access and connectivity to all Cortex XDR agents

The disk space requirement is based on the number of agents and the frequency of content updates. The Broker VM stores the content updates locally and distributes them to the agents. The disk space also depends on the retention period of the content updates, which can be configured in the Broker VM settings. The default retention period is 30 days.

Broker VM for Cortex XDR

PCDRA Study Guide

Question 9

Question Type: MultipleChoice

What is the purpose of targeting software vendors in a supply-chain attack?

Options:

A- to take advantage of a trusted software delivery method.

B- to steal users' login credentials.

C- to access source code.

D- to report Zero-day vulnerabilities.

Answer:

A

Explanation:

A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Software supply chain attacks inject malicious code into an application in order to infect all users of an app. The purpose of targeting software vendors in a supply-chain attack is to take advantage of a trusted software delivery method, such as an update or a download, that can reach a large number of potential victims. By compromising a software vendor, an attacker can bypass the security measures of the downstream organizations and gain access to their systems, data, or networks.Reference:

What Is a Supply Chain Attack? - Definition, Examples & More | Proofpoint US

What Is a Supply Chain Attack? - CrowdStrike

What Is a Supply Chain Attack? | Zscaler

What Is a Supply Chain Attack? Definition, Examples & Prevention

To Get Premium Files for PCDRA Visit

https://www.p2pexams.com/products/pcdra

For More Free Questions Visit

https://www.p2pexams.com/palo-alto-networks/pdf/pcdra

20%
DISCOUNT