PCDRA$^{\text{Q\&As}}$

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

QUESTION 1

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder

B. Local Agent Proxy

C. Local Agent Installer and Content Caching

D. Broker VM Syslog Collector

Correct Answer: B

Explanation: If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it here1 and here2. References: Local Agent Proxy Configure the Local Agent Proxy Setup

QUESTION 2

Which profiles can the user use to configure malware protection in the Cortex XDR console?

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

Correct Answer: A

Explanation: The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. References: Malware Protection Profile Endpoint Security Policy

QUESTION 3

How can you pivot within a row to Causality view and Timeline views for further investigate?

A. Using the Open Card Only

B. Using the Open Card and Open Timeline actions respectively

C. You can\\'t pivot within a row to Causality view and Timeline views

D. Using Open Timeline Actions Only

Correct Answer: B

Explanation: To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident. References: Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

QUESTION 4

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within athree-hourtime frame are grouped together into one Incident.

C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D. Every alert creates a new Incident.

Correct Answer: C

Explanation: The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details1. Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack. Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack. Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes. References: Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2 Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

QUESTION 5

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 6

When is the wss (WebSocket Secure) protocol used?

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

Correct 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 CortexXDR 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. References: 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 (QandA) 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 7

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

A. Agent Proxy

B. Agent Installer and Content Caching

C. Syslog Collector

D. CSV Collector

Correct 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. References: Agent Installer and Content Caching Install an SSL Certificate on the Broker VM

QUESTION 8

Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

A. Search and destroy

B. Isolation

C. Quarantine

D. Flag for removal

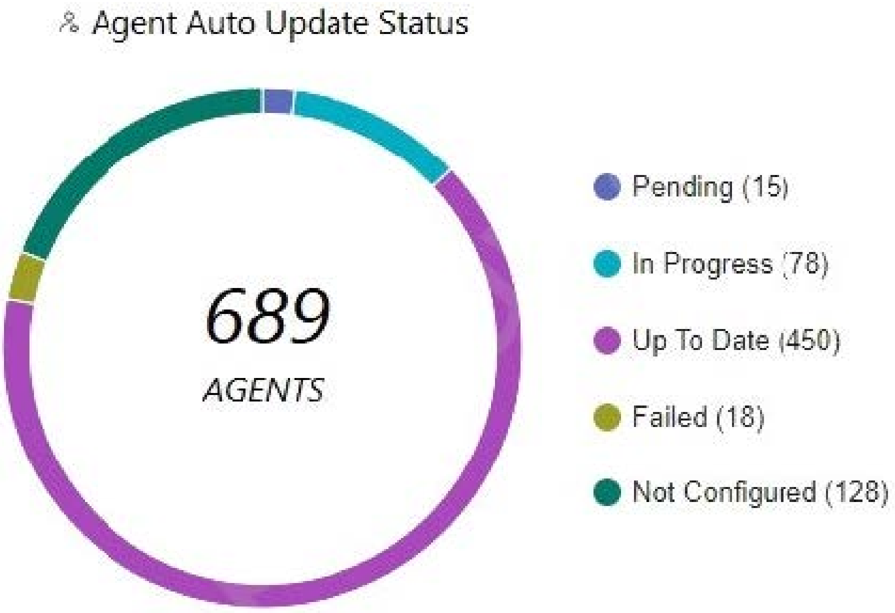
Correct Answer: C

Explanation: The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension.

You can view, restore, or delete the quarantined files from the Cortex XDR console. References: Quarantine Files Manage Quarantined Files

QUESTION 9

Which statement is true based on the following Agent Auto Upgrade widget?



A. There are a total of 689 Up To Date agents.

B. Agent Auto Upgrade was enabled but not on all endpoints.

C. Agent Auto Upgrade has not been enabled.

D. There are more agents in Pending status than In Progress status.

Correct Answer: B

Explanation: The Agent Auto Upgrade widget shows the status of the agent auto upgrade feature on the endpoints. The widget displays the number of agents that are up to date, in progress, pending, failed, and not configured. In this case,

the widget shows that there are 450 agents that are up to date, 78 in progress, 15 pending, 18 failed, and 128 not configured. This means that the agent auto upgrade feature was enabled but not on all endpoints. References:

Cortex XDR Agent Auto Upgrade

PCDRA Study Guide

QUESTION 10

Can you disable the ability to use the Live Terminal feature in Cortex XDR?

A. Yes, via the Cortex XDR console or with an installation switch.

B. No, a separate installer package without Live Terminal is required.

C. No, it is a required feature of the agent.

D. Yes, via Agent Settings Profile.

Correct Answer: D

Explanation: The Live Terminal feature in Cortex XDR allows you to initiate a remote connection to an endpoint and perform various actions such as running commands, uploading and downloading files, and terminating processes. You can disable the ability to use the Live Terminal feature in Cortex XDR by configuring the Agent Settings Profile. The Agent Settings Profile defines the behavior and functionality of the Cortex XDR agent on the endpoint. You can create different profiles for different groups of endpoints and assign them accordingly. To disable the Live Terminal feature, you need to uncheck the Enable Live Terminal option in the Agent Settings Profile and save the changes. This will prevent the Cortex XDR agent from accepting any Live Terminal requests from the Cortex XDR management console. References: Live Terminal: This document explains how to use the Live Terminal feature to investigate and respond to security events on Windows endpoints. Agent Settings Profile: This document describes how to create and manage Agent Settings Profiles to define the behavior and functionality of the Cortex XDR agent on the endpoint.

QUESTION 11

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

A. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

B. Enable DLL Protection on all servers but there might be some false positives.

C. Create IOCs of the malicious files you have found to prevent their execution.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Correct Answer: A

Explanation: To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create

custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to

define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers12.

Let\\'s briefly discuss the other options to provide a comprehensive explanation:

B. Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted3. C. Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection4.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not have an option to enable or configure BTP rules. In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply chain attack. References: Behavioral Threat Protection Create a BTP Rule DLL Protection Create an IOC Rule [Cytool]

QUESTION 12

When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

A. Pending

B. It is blank

C. Unassigned

D. New

Correct Answer: C

Explanation: The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule12. Let\\'s briefly discuss the other options to provide a comprehensive explanation:

A. Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as

"New", "Active", "Done", "Closed", or "Pending"3.

B. It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group12.
D. New:

This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done",

"Closed", or "Pending"3.

In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.

References:

Cortex XDR Pro Admin Guide: Manage Incidents

Cortex XDR Pro Admin Guide: Assign Incidents

Cortex XDR Pro Admin Guide: Update Incident Status

QUESTION 13

When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

A. The agent technical support file.

B. The prevention archive from the alert.

C. The distribution id of the agent.

D. A list of all the current exceptions applied to the agent.

E. The unique agent id.

Correct Answer: AB

Explanation: When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are: The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself. The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself. The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example: The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder. A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent\\'s security policies. The exceptions can help TAC understand the agent\\'s configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file. The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file. References: Generate and Download the Agent Technical Support File Generate and Download the Prevention Archive Cortex XDR Agent Administrator Guide: Agent Distribution ID Cortex XDR Agent Administrator Guide: Exception Security Profiles [Cortex XDR Agent Administrator Guide: Unique Agent ID]

QUESTION 14

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 15

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