PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

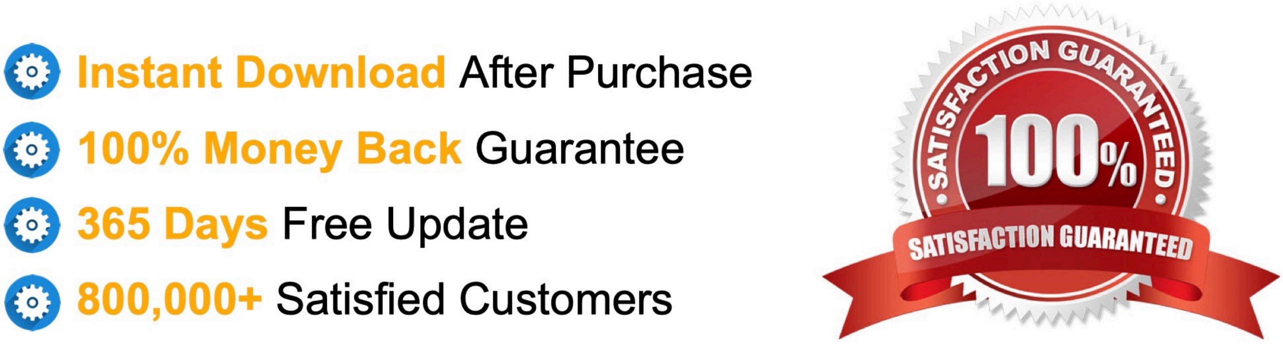
Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

Correct Answer: D

Explanation: When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. References: Remediation Suggestions Apply Remediation Suggestions

QUESTION 2

In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

A. Salesforce

B. Jira

C. Service Now

D. Slack

Correct Answer: D

Explanation: Cortex XDR allows you to schedule reports and forward them to Slack, a cloud-based collaboration platform. You can configure the Slack channel, frequency, and recipients of the scheduled reports. You can also view the report

history and status in the Cortex XDR management console. References:

Scheduled Queries: This document explains how to create, edit, and manage scheduled queries and reports in Cortex XDR.

Forward Scheduled Reports to Slack: This document provides the steps to configure Slack integration and forward scheduled reports to a Slack channel.

QUESTION 3

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

A. Automatically close the connections involved in malicious traffic.

B. Automatically kill the processes involved in malicious activity.

C. Automatically terminate the threads involved in malicious activity.

D. Automatically block the IP addresses involved in malicious traffic.

Correct Answer: BD

Explanation: The "Respond to Malicious Causality Chains" feature in a Cortex XDR Windows Malware profile allows the agent to take automatic actions against network connections and processes that are involved in malicious activity on the

endpoint. The feature has two modes: Block IP Address and Kill Process1. The two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile are:

Automatically kill the processes involved in malicious activity. This can help to stop the malware from spreading or doing any further damage. Automatically block the IP addresses involved in malicious traffic. This can help to prevent the

malware from communicating with its command and control server or other malicious hosts.

The other two options, automatically close the connections involved in malicious traffic and automatically terminate the threads involved in malicious activity, are not specific to "Respond to Malicious Causality Chains". They are general

security measures that the agent can perform regardless of the feature.

References:

Cortex XDR Agent Security Profiles

Cortex XDR Agent 7.5 Release Notes

PCDRA: What are purposes of "Respond to Malicious Causality Chains" in ...

QUESTION 4

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.

B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.

C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.

Correct Answer: D

Explanation: To add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint, you need to use the Action Center in Cortex XDR. The Action Center allows you to create and manage actions that apply to endpoints, such as adding files or processes to the allow list or block list, isolating or unisolating endpoints, or initiating live terminal sessions. To add a file hash to the allow list, you need to choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it. This will prevent the Malware profile from scanning or blocking the file on the endpoints that match the scope of the action. References: Cortex XDR 3: Responding to Attacks1, Action Center2

QUESTION 5

Which statement regarding scripts in Cortex XDR is true?

A. Any version of Python script can be run.

B. The level of risk is assigned to the script upon import.

C. Any script can be imported including Visual Basic (VB) scripts.

D. The script is run on the machine uploading the script to ensure that it is operational.

Correct Answer: B

Explanation: The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk

determines the permissions and restrictions for running the script on endpoints. The levels of risk are:

Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.

The other options are incorrect for the following reasons:

A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts

must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.

C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation.

VB scripts are not supported by Cortex XDR, and will not run on the endpoints. D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and

size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.

References:

Agent Script Library

Import a Script

Run Scripts on an Endpoint

QUESTION 6

In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

B. Create a new rule exception and use the singer as the characteristic.

C. Add the signer to the allow list in the malware profile.

D. Add the signer to the allow list under the action center page.

Correct Answer: C

Explanation: To prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. A

malware profile is a profile that defines the settings and actions for malware prevention and detection on the endpoints. A malware profile allows you to specify a list of files, folders, or signers that you want to exclude from malware scanning

and blocking. By adding the signer to the allow list in the malware profile, you can prevent the Cortex XDR Agent from blocking any file that is signed by that signer1.

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

A. In the Restrictions Profile, add the file name and path to the Executable Files allow list: This is not the correct answer. Adding the file name and path to the Executable Files allow list in the Restrictions Profile will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A Restrictions Profile is a profile that defines the settings and actions for restricting the execution of files or processes on the endpoints. A Restrictions Profile allows you to specify a list of executable files that you want to allow or block based on the file name and path. However, this method does not take into account the digital signer of the file, and it may not be effective if the file name or path changes2. B. Create a new rule exception and use the signer as the characteristic: This is not the correct answer. Creating a new rule exception and using the signer as the characteristic will not prevent theCortex XDR Agent from blocking execution of a file based on the digital signer. A rule exception is an exception that you can create to modify the behavior of a specific prevention rule or BIOC rule. A rule exception allows you to specify the characteristics and the actions that you want to apply to the exception, such as file hash, process name, IP address, or domain name. However, this method does not support using the signer as a characteristic, and it may not be applicable to all prevention rules or BIOC rules3.

D. Add the signer to the allow list under the action center page: This is not the correct answer. Adding the signer to the allow list under the action center page will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. The action center page is a page that allows you to create and manage actions that you can perform on your endpoints, such as isolating, scanning, collecting files, or executing scripts. The action center page does not have an option to add a signer to the allow list, and it is not related to the malware prevention or detection functionality4. In conclusion, to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. By using this method, you can exclude the files that are signed by the trusted signer from the malware scanning and blocking. References: Add a New Malware Security Profile Add a New Restrictions Security Profile Create a Rule Exception Action Center

QUESTION 7

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 8

What types of actions you can execute with live terminal session?

A. Manage Network configurations, Quarantine Files, Run PowerShell scripts

B. Manage Processes, Manage Files, Run Operating System Commands, Run Ruby Commands and Scripts

C. Apply patches, Reboot System, send notification for end user, Run Python Commands and Scripts

D. Manage Processes, Manage Files, Run Operating System Commands, Run Python Commands and Scripts

Correct Answer: D

Explanation: Live terminal session is a feature of Cortex XDR that allows you to remotely access and control endpoints from the Cortex XDR console. With live terminal session, you can execute various actions on the endpoints, such as: Manage Processes: You can view, start, or kill processes on the endpoint, and monitor their CPU and memory usage. Manage Files: You can view, create, delete, or move files and folders on the endpoint, and upload or download files to or from the endpoint. Run Operating System Commands: You can run commands on the endpoint using the native command-line interface of the operating system, such as cmd.exe for Windows, bash for Linux, or zsh for macOS. Run Python Commands and Scripts: You can run Python commands and scripts on the endpoint using the Python interpreter embedded in the Cortex XDR agent. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint. References: Initiate a Live Terminal Session Manage Processes Manage Files Run Operating System Commands Run Python Commands and Scripts

QUESTION 9

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Correct Answer: AB

Explanation: When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 References: Assign Incidents to an Analyst in Bulk Change the Status of Multiple Incidents

QUESTION 10

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

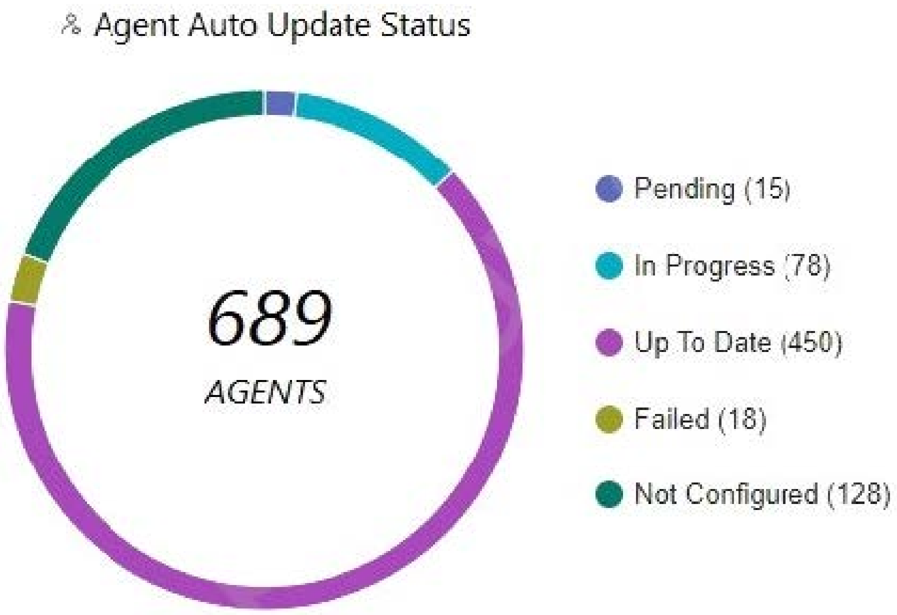
Explanation: Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and 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 11

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 12

What should you do to automatically convert leads into alerts after investigating a lead?

A. Lead threats can\\'t be prevented in the future because they already exist in the environment.

B. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

C. Create BIOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

D. Build a search query using Query Builder or XQL using a list of lOCs.

Correct Answer: B

Explanation: To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. References: PCDRA Study Guide, page 25 Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2 Cortex XDR Documentation, section "Create IOC Rules"

QUESTION 13

Which type of BIOC rule is currently available in Cortex XDR?

A. Threat Actor

B. Discovery

C. Network

D. Dropper

Correct Answer: B

Explanation: The type of BIOC rule that is currently available in Cortex XDR is Discovery. A Discovery BIOC rule is a rule that detects suspicious or malicious behavior on endpoints based on the Cortex XDR data. A Discovery BIOC rule can

use various event types, such as file, injection, load image, network, process, registry, or user, to define the criteria for the rule. A Discovery BIOC rule can also use operators, functions, and variables to create complex logic and conditions for

the rule. A Discovery BIOC rule can generate alerts when the rule is triggered, and these alerts can be grouped into incidents for further investigation and response12.

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

A. Threat Actor: This is not the correct answer. Threat Actor is not a type of BIOC rule that is currently available in

Cortex XDR. Threat Actor is a term that refers to an individual or a group that is responsible for a cyberattack or a threat campaign. Cortex XDR does not support creating BIOC rules based on threat actors, but it can provide threat intelligence and context from various sources, such as Unit 42, AutoFocus, or Cortex XSOAR3. C. Network: This is not the correct answer. Network is not a type of BIOC rule that is currently available in Cortex XDR. Network is an event type that can be used in a Discovery BIOC rule to define the criteria based on network attributes, such as source IP, destination IP, source port, destination port, protocol, or domain. Network is not a standalone type of BIOC rule, but a part of the Discovery BIOC rule2. D. Dropper: This is not the correct answer. Dropper is not a type of BIOC rule that is currently available in Cortex XDR. Dropper is a term that refers to a type of malware that is designed to download and install other malicious files or programs on a compromised system. Cortex XDR does not support creating BIOC rules based on droppers, but it can detect and prevent droppers using various methods, such as behavioral threat protection, exploit prevention, or WildFire analysis4. In conclusion, the type of BIOC rule that is currently available in Cortex XDR is Discovery. By using Discovery BIOC rules, you can create custom detection rules that match your specific use cases and scenarios. References: Create a BIOC Rule BIOC Rule Event Types Threat Intelligence and Context Malware Prevention

QUESTION 14

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 15

What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

A. MTH researches for threats in the tenant and generates a report with the findings.

B. MTH researches for threats in the logs and reports to engineering.

C. MTH runs queries and investigative actions and no further action is taken.

D. MTH pushes content updates to prevent against thezero-dayexploits.

Correct Answer: A

Explanation: The Managed Threat Hunting (MTH) team is a group of security experts who proactively hunt for threats in the Cortex XDR tenant and generate a report with the findings. The MTH team uses advanced queries and investigative actions to identify and analyze potential threats, such as zero-day exploits, that may have bypassed the prevention and detection capabilities of Cortex XDR. The MTH team also provides recommendations and best practices to help customers remediate the threats and improve their security posture. References: Managed Threat Hunting Service Managed Threat Hunting Report