# 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.passapply.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**

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 2**

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

**QUESTION 3**

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

A. mark the incident as Unresolved

B. create a BIOC rule excluding this behavior

C. create an exception to prevent future false positives

D. mark the incident as Resolved -False Positive

Correct Answer: D

Explanation: If all alerts contained in a Cortex XDR incident have exclusions, the Cortex XDR console will automatically mark the incident as Resolved ?False Positive. This means that the incident was not a real threat, but a benign or legitimate activity that triggered an alert. By marking the incident as Resolved?False Positive, the Cortex XDR console removes the incident from the list of unresolved incidents and does not count it towards the incident statistics. This helps the analyst to focus on the true positive incidents that require further investigation and response1. An exclusion is a rule that hides an alert from the Cortex XDR console, based on certain criteria, such as the alert source, type, severity, or description. An exclusion does not change the security policy or prevent the alert from firing, it only suppresses the alert from the console. An exclusion is useful when the analyst wants to reduce the noise of false positive alerts that are not relevant or important2. An exception, on the other hand, is a rule that overrides the security policy and allows or blocks a process or file from running on an endpoint, based on certain attributes, such as the file hash, path, name, or signer. An exception is useful when the analyst wants to prevent false negative alerts that are caused by malicious or unwanted files or processes that are not detected by the security policy3. A BIOC rule is a rule that creates an alert based on a custom XQL query that defines a specific behavior of interest or concern. A BIOC rule is useful when the analyst wants to detect and alert on anomalous or suspicious activities that are not covered by the default Cortex XDR rules4. References: Palo Alto Networks Cortex XDR Documentation, Resolve an Incident1 Palo Alto Networks Cortex XDR Documentation, Alert Exclusions2 Palo Alto Networks Cortex XDR Documentation, Exceptions3 Palo Alto Networks Cortex XDR Documentation, BIOC Rules4

**QUESTION 4**

The Cortex XDR console has triggered an incident, blocking a vitally important piece of software in your organization that is known to be benign. Which of the following options would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization?

A. Create an individual alert exclusion.

B. Create a global inclusion.

C. Create an endpoint-specific exception.

D. Create a global exception.

Correct Answer: D

Explanation: A global exception is a rule that allows you to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR. A global exception applies to all endpoints in your organization that are protected by

Cortex XDR. Creating a global exception for a vitally important piece of software that is known to be benign would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization.

To create a global exception, you need to follow these steps:

In the Cortex XDR management console, go to Policy Management > Exceptions and click Add Exception.

Select the Global Exception option and click Next. Enter a name and description for the exception and click Next. Select the type of exception you want to create, such as file, process, or behavior, and click Next.

Specify the criteria for the exception, such as file name, hash, path, process name, command line, or behavior name, and click Next.

Review the summary of the exception and click Finish.

References:

Create Global Exceptions: This document explains how to create global exceptions to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR.

Exceptions Overview: This document provides an overview of exceptions and how they can be used to fine-tune the Cortex XDR security policy.

**QUESTION 5**

What is the difference between presets and datasets in XQL?

A. A dataset is a Cortex data lake data source only; presets are built-in data source.

B. A dataset is a built-in orthird-partysource; presets group XDR data fields.

C. A dataset is a database; presets is a field.

D. A dataset is a third-party data source; presets are built-in data source.

Correct Answer: B

Explanation: The difference between presets and datasets in XQL is that a dataset is a built-in or third-party data source, while a preset is a group of XDR data fields. A dataset is a collection of data that you can query and analyze using XQL.

A dataset can be a Cortex data lake data source, such as endpoints, alerts, incidents, or network flows, or a third- party data source, such as AWS CloudTrail, Azure Activity Logs, or Google Cloud Audit Logs. A preset is a predefined set of

XDR data fields that are relevant for a specific use case, such as process execution, file operations, or network activity. A preset can help you simplify and standardize your XQL queries by selecting the most important fields for youranalysis.

You can use presets with any Cortex data lake data source, but not with third-party data sources. References:

Datasets and Presets

XQL Language Reference