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

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 2

Which of the following Live Terminal options are available for Android systems?

A. Live Terminal is not supported.

B. Stop an app.

C. Run APK scripts.

D. Run Android commands.

Correct Answer: D

Explanation: Cortex XDR supports Live Terminal for Android systems, which allows you to remotely access and manage Android endpoints using a command-line interface. You can use Live Terminal to run Android commands, such as adb shell, adb logcat, adb install, and adb uninstall. You can also use Live Terminal to view and modify files, directories, and permissions on the Android endpoints. Live Terminal for Android systems does not support stopping an app or running APK scripts. References: Cortex XDR documentation portal Initiate a Live Terminal Session Live Terminal Commands

QUESTION 3

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

QUESTION 4

What motivation do ransomware attackers have for returning access to systems once their victims have paid?

A. There is organized crime governance among attackers that requires the return of access to remain in good standing.
B. Nation-states enforce the return of system access through the use of laws and regulation.

B. Failure to restore access to systems undermines the scheme because others will not believe their valuables would be returned.

C. The ransomware attackers hope to trace the financial trail back and steal more from traditional banking institutions.

Correct Answer: C

Explanation: Ransomware attackers have a motivation to return access to systems once their victims have paid because they want to maintain their reputation and credibility. If they fail to restore access to systems, they risk losing the trust of future victims who may not believe that paying the ransom will result in getting their data back. This would reduce the effectiveness and profitability of their scheme. Therefore, ransomware attackers have an incentive to honor their promises and decrypt the data after receiving the ransom. References: What is the motivation behind ransomware? | Foresite As Ransomware Attackers\\' Motives Change, So Should Your Defense - Forbes

QUESTION 5

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