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.geekcert.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 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 2

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

A. Enable DLL Protection on all endpoints but there might be some false positives.

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

C. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.

D. No step is required because the malicious document is already stopped.

Correct Answer: B

Explanation: The correct answer is B, create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP rules are a powerful feature of Cortex XDR that allow you to define custom rules to detect and block malicious behaviors on endpoints. You can use BTP rules to create indicators of compromise (IOCs) based on file attributes, registry keys, processes, network connections, and other criteria. By creating BTP rules, you can prevent the same malicious Word document from being opened by other users in your organization, even if the document has a different name or hash value. BTP rules are updated through content updates and can be managed from the Cortex XDR console. The other options are incorrect for the following reasons: A is incorrect because enabling DLL Protection on all endpoints is not a specific or effective way to prevent the malicious Word document. DLL Protection is a feature of Cortex XDR that prevents the loading of unsigned or untrusted DLLs by protected processes. However, this feature does not apply to Word documents or macros, and may cause false positives or compatibility issues with legitimate applications. C is incorrect because relying on Cortex to share IOCs with the Cyber Threat Alliance members is not a proactive or sufficient way to prevent the malicious Word document. The Cyber Threat Alliance is a group of cybersecurity vendors that share threat intelligence and best practices to improve their products and services. However, not all vendors are members of the alliance, and not all IOCs are shared or updated in a timely manner. Therefore, you cannot assume that other users in your organization are protected by the same IOCs as Cortex XDR. D is incorrect

because doing nothing is not a responsible or secure way to prevent the malicious Word document. Even though Cortex XDR agent prevented the attempt to open the document on one endpoint, it does not mean that the document is no longer a threat. The document may still be circulating in your network or email system, and may be opened by other users who have different agent profiles or policies. Therefore, you should take steps to identify and block the document across your organization. References: Cortex XDR Agent Administrator Guide: Behavioral Threat Protection Cortex XDR Agent Administrator Guide: DLL Protection Palo Alto Networks: Cyber Threat Alliance

QUESTION 3

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.

B. It is false positive.

C. It is a false negative.

D. It is true negative.

Correct Answer: B

Explanation: A false positive is a situation where a file or activity is incorrectly identified as malicious by a security tool, when in fact it is benign or harmless. A false positive can cause unnecessary alerts, disruptions, or remediation actions, and reduce the confidence and efficiency of the security system. In this question, a file is identified as malware by the Local Analysis module, whereas WildFire verdict is Benign, assuming WildFire is accurate. This means that the Local Analysis module has made a mistake and flagged a legitimate file as malicious, while WildFire has correctly determined that the file is safe. Therefore, this is an example of a false positive. The Local Analysis module is a feature of the Cortex XDR agent that uses a static set of pattern-matching rules and a statistical model to determine if an unknown file is likely to be malware. The Local Analysis module can provide a fast and offline verdict for files that are not yet analyzed by WildFire, but it is not as accurate or comprehensive as WildFire, which uses dynamic analysis and machine learning to examine the behavior and characteristics of files in a sandbox environment. WildFire verdicts are considered more reliable and authoritative than Local Analysis verdicts, and can override them in case of a discrepancy. Therefore, if a file is identified as malware by the Local Analysis module, but as Benign by WildFire, the WildFire verdict should be trusted and the Local Analysis verdict should be disregarded123 References: False positive (security) - Wikipedia Local Analysis WildFire Overview

QUESTION 4

You can star security events in which two ways? (Choose two.)

A. Create an alert-starring configuration.

B. Create an Incident-starring configuration.

C. Manually star an alert.

D. Manually star an Incident.

Correct Answer: CD

Explanation: You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you prioritize and track the events that are

most important to you. You can also filter and sort the events by their star status in the Cortex XDR console. To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again. To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed. References: Star Security Events Create an Alert Starring Configuration Create an Incident Starring Configuration

QUESTION 5

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