CertsDeals

Free Questions for PCDRA by certsdeals

Shared by Hill on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

Options:

A- causality_chain

B- endpoint_name

C- threat_event

D- event_type

Answer:

D

Explanation:

To create a BIOC rule with XQL query, you must at a minimum filter on theevent_typefield in order for it to be a valid BIOC rule. The event_type field indicates the type of event that triggered the alert, such as PROCESS, FILE, REGISTRY, NETWORK, or

USER_ACCOUNT. Filtering on this field helps you narrow down the scope of your query and focus on the relevant events for your use case. Other fields, such as causality_chain, endpoint_name, threat_event, are optional and can be used to further refine your query or display additional information in the alert.Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9

Palo Alto Networks Cortex XDR Documentation, BIOC Rule Query Syntax

Question 2

Question Type: MultipleChoice

Which statement is true for Application Exploits and Kernel Exploits?

Options:

A- The ultimate goal of any exploit is to reach the application.

B- Kernel exploits are easier to prevent then application exploits.

C- The ultimate goal of any exploit is to reach the kernel.

D- Application exploits leverage kernel vulnerability.

Answer:

C

Explanation:

The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than application exploits, because they can bypass security mechanisms and hide their presence from the user and the system.Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8

Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

Question 3

Question Type: **MultipleChoice**

What is the outcome of creating and implementing an alert exclusion?

Options:

A- The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

B- The Cortex XDR console will hide those alerts.

C- The Cortex XDR agent will not create an alert for this event in the future.

D- The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Answer:

B

Explanation:

The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint.Therefore, the correct answer is B, the Cortex XDR console will hide those alerts12

Alert Exclusions

Create an Alert Exclusion Policy

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- It is true positive.

B- It is false positive.

C- It is a false negative.

D- It is true negative.

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

False positive (security) - Wikipedia

Local Analysis

WildFire Overview

Question 5

Question Type: **MultipleChoice**

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

Options:

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.

Answer:

A, B

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

Assign Incidents to an Analyst in Bulk

Change the Status of Multiple Incidents

Question 6

Question Type: **MultipleChoice**

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques.

Options:

A- Exfiltration, Command and Control, Collection

B- Exfiltration, Command and Control, Privilege Escalation

C- Exfiltration, Command and Control, Impact

D- Exfiltration, Command and Control, Lateral Movement

Answer:

D

Explanation:

Cortex XDR Analytics is a feature of Cortex XDR that leverages machine learning and behavioral analytics to detect and alert on malicious activity across the network and endpoint layers. Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques: Exfiltration, Command and Control, Lateral Movement, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection. However, among the options given in the question, the correct answer is D, Exfiltration, Command and Control, Lateral Movement. These are three of the most critical techniques that indicate an advanced and persistent threat (APT) in the environment. Exfiltration refers to the technique of transferring data or information from the compromised system or network to an external location controlled by the adversary. Command and Control refers to the technique of communicating with the compromised system or network to provide instructions, receive data, or update malware. Lateral Movement refers to the technique of moving from one system or network to another within the same environment, usually to gain access to more resources or data. Cortex XDR Analytics can alert on these techniques by analyzing various data sources, such as network traffic, firewall logs, endpoint events, and threat intelligence, and applying behavioral models, anomaly detection, and correlation rules.Cortex XDR Analytics can also map the alerts to the corresponding MITRE ATT&CKTM techniques and provide additional context and visibility into the attack chain1234

Cortex XDR Analytics

MITRE ATT&CKTM

Cortex XDR Analytics MITRE ATT&CKTM Techniques

Cortex XDR Analytics Alert Categories

Question 7

Question Type: **MultipleChoice**

What is by far the most common tactic used by ransomware to shut down a victim's operation?

Options:

A- preventing the victim from being able to access APIs to cripple infrastructure

B- denying traffic out of the victims network until payment is received

C- restricting access to administrative accounts to the victim

D- encrypting certain files to prevent access by the victim

Answer:

D

Explanation:

Ransomware is a type of malicious software, or malware, that encrypts certain files or data on the victim's system or network and prevents them from accessing their data until they pay a ransom. This is by far the most common tactic used by ransomware to shut down a victim's operation, as it can cause costly disruptions, data loss, and reputational damage. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again.Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack1234

What is Ransomware? | How to Protect Against Ransomware in 2023

Ransomware - Wikipedia

What is ransomware? | Ransomware meaning | Cloudflare

[What Is Ransomware? | Ransomware.org]

[Ransomware --- FBI]

Question 8

Question Type: **MultipleChoice**

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?

Options:

A- Broker VM Pathfinder

B- Local Agent Proxy

C- Local Agent Installer and Content Caching

D- Broker VM Syslog Collector

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 here1and here2.Reference:

Local Agent Proxy

Configure the Local Agent Proxy Setup

Question 9

Question Type: **MultipleChoice**

When using the ''File Search and Destroy'' feature, which of the following search hash type is supported?

Options:

A- SHA256 hash of the file

B- AES256 hash of the file

C- MD5 hash of the file

D- SHA1 hash of the file

Answer:

A

Explanation:

The File Search and Destroy feature is a capability of Cortex XDR that allows you to search for and delete malicious or unwanted files across your endpoints. You can use this feature to quickly respond to incidents, remediate threats, and enforce compliance policies. To use the File Search and Destroy feature, you need to specify the file name and the file hash of the file you want to search for and delete. The file hash is a unique identifier of the file that is generated by a cryptographic hash function. The file hash ensures that you are targeting the exact file you want, and not a file with a similar name or a different version. The File Search and Destroy feature supports the SHA256 hash type, which is a secure hash algorithm that produces a 256-bit (32-byte) hash value. The SHA256 hash type is widely used for file integrity verification and digital signatures. The File Search and Destroy feature does not support other hash types, such as AES256, MD5, or SHA1, which are either encryption algorithms or less secure hash algorithms.Therefore, the correct answer is A, SHA256 hash of the file1234

File Search and Destroy

What is a File Hash?

SHA-2 - Wikipedia

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

Question 10

Question Type: **MultipleChoice**

What kind of the threat typically encrypts user files?

Options:

A- ransomware

B- SQL injection attacks

C- Zero-day exploits

D- supply-chain attacks

Answer:

A

Explanation:

Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again.Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack123456

What is Ransomware? | How to Protect Against Ransomware in 2023

Ransomware - Wikipedia

What is ransomware? | Ransomware meaning | Cloudflare

What Is Ransomware? | Ransomware.org

Ransomware --- FBI

To Get Premium Files for PCDRA Visit

https://www.p2pexams.com/products/pcdra

For More Free Questions Visit

https://www.p2pexams.com/palo-alto-networks/pdf/pcdra