Free Questions for PCDRA by certsinside

Shared by Spence on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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 IOCs.

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.Reference:

PCDRA Study Guide, page 25

Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2

Cortex XDR Documentation, section "Create IOC Rules"

Question 2

Question Type: MultipleChoice

What is the difference between presets and datasets in XQL?

Options:

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

B- A dataset is a built-in or third-party source; 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.

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

Datasets and Presets

XQL Language Reference

Question 3

Question Type: **MultipleChoice**

Cortex XDR is deployed in the enterprise and you notice a cobalt strike attack via an ongoing supply chain compromise was prevented on 1 server. What steps can you take to ensure the same protection is extended to all your servers?

Options:

A- Conduct a thorough Endpoint Malware scan.

B- Enable DLL Protection on all servers but there might be some false positives.

C- Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

D- Create lOCs of the malicious files you have found to prevent their execution.

Answer:

D

Explanation:

The best step to ensure the same protection is extended to all your servers is to create indicators of compromise (IOCs) of the malicious files you have found to prevent their execution. IOCs are pieces of information that indicate a potential threat or compromise on an endpoint, such as file hashes, IP addresses, domain names, or registry keys. You can create IOCs in Cortex XDR to block or alert on any file or network activity that matches the IOCs. By creating IOCs of the malicious files involved in the cobalt strike attack, you can prevent them from running or spreading on any of your servers.

The other options are not the best steps for the following reasons:

A is not the best step because conducting a thorough Endpoint Malware scan may not detect or prevent the cobalt strike attack if the malicious files are obfuscated, encrypted, or hidden. Endpoint Malware scan is a feature of Cortex XDR that allows you to scan endpoints for known malware and quarantine any malicious files found. However, Endpoint Malware scan may not be effective against unknown or advanced threats that use evasion techniques to avoid detection.

B is not the best step because enabling DLL Protection on all servers may cause some false positives and disrupt legitimate applications. DLL Protection is a feature of Cortex XDR that allows you to block or alert on any DLL loading activity that matches certain criteria, such as unsigned DLLs, DLLs loaded from network locations, or DLLs loaded by specific processes. However, DLL Protection may also block or alert on benign DLL loading activity that is part of normal system or application operations, resulting in false positives and performance issues.

C is not the best step because enabling Behavioral Threat Protection (BTP) with cytool may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection. Behavioral Threat Protection is a feature of Cortex XDR that allows you to block or alert on any endpoint behavior that matches certain patterns, such as ransomware, credential theft, or lateral movement. Cytool is a command-line tool that allows you to configure and manage the Cortex XDR agent on the endpoint. However, Behavioral Threat Protection may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection, such as encryption, obfuscation, or proxy servers.

Create IOCs

Scan an Endpoint for Malware

DLL Protection

Behavioral Threat Protection

Cytool for Windows

Question 4

Question Type: MultipleChoice

To stop a network-based attack, any interference with a portion of the attack pattern is enough to prevent it from succeeding. Which statement is correct regarding the Cortex XDR Analytics module?

Options:

A- It does not interfere with any portion of the pattern on the endpoint.

B- It interferes with the pattern as soon as it is observed by the firewall.

C- It does not need to interfere with the any portion of the pattern to prevent the attack.

D- It interferes with the pattern as soon as it is observed on the endpoint.

Answer:

D

Explanation:

The correct statement regarding the Cortex XDR Analytics module is D, it interferes with the pattern as soon as it is observed on the endpoint. The Cortex XDR Analytics module is a feature of Cortex XDR that uses machine learning and behavioral analytics to detect and prevent network-based attacks on endpoints. The Cortex XDR Analytics module analyzes the network traffic and activity on the endpoint, and compares it with the attack patterns defined by Palo Alto Networks threat research team. The Cortex XDR Analytics module interferes with the attack pattern as soon as it is observed on the endpoint, by blocking the malicious network connection, process, or file. This way, the Cortex XDR Analytics module can stop the attack before it causes any damage or compromise.

The other statements are incorrect for the following reasons:

A is incorrect because the Cortex XDR Analytics module does interfere with the attack pattern on the endpoint, by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on the firewall or any other network device to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.

B is incorrect because the Cortex XDR Analytics module does not interfere with the attack pattern as soon as it is observed by the firewall. The Cortex XDR Analytics module does not depend on the firewall or any other network device to detect or prevent the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the analysis and interference. The firewall may not be able to observe or block the attack pattern if it is encrypted, obfuscated, or bypassed by the attacker.

C is incorrect because the Cortex XDR Analytics module does need to interfere with the attack pattern to prevent the attack. The Cortex XDR Analytics module does not only detect the attack pattern, but also prevents it from succeeding by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on any other response mechanism or human intervention to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.

Cortex XDR Analytics Module Detection and Prevention

Question 5

Question Type: MultipleChoice

Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

Options:

A- Search & destroy

B- Isolation

C- Quarantine

D- Flag for removal

Answer:

C

Explanation:

The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed isquarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console.Reference:

Quarantine Files

Manage Quarantined Files

Question 6

Question Type: **MultipleChoice**

What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

Options:

A- Ransomware

B- Worm

C- Keylogger

D- Rootkit

Answer:

A

Explanation:

The kind of malware that uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim isransomware. Ransomware is a type of malware that encrypts the victim's files or blocks access to their system, and then demands a ransom for the decryption key or the restoration of access. Ransomware can also threaten to expose or delete the victim's data if the ransom is not paid. Ransomware can cause significant damage and disruption to individuals, businesses, and organizations, and can be difficult to remove or recover from. Some examples of ransomware are CryptoLocker, WannaCry, Ryuk, and REvil.

12 Types of Malware + Examples That You Should Know - CrowdStrike

What is Malware? Malware Definition, Types and Protection

12+ Types of Malware Explained with Examples (Complete List)

Question 7

Question Type: MultipleChoice

Which version of python is used in live terminal?

Options:

A- Python 2 and 3 with standard Python libraries

B- Python 2 and 3 with specific XDR Python libraries developed by Palo Alto Networks

C- Python 3 with specific XDR Python libraries developed by Palo Alto Networks

D- Python 3 with standard Python libraries

Answer:

D

Explanation:

Live terminal uses Python 3 with standard Python libraries to run Python commands and scripts on the endpoint. Live terminal does not support Python 2 or any custom or external Python libraries. Live terminal uses the Python interpreter embedded in the Cortex XDR

agent, which is based on Python 3.7.4. The standard Python libraries are the modules that are included with the Python installation and provide a wide range of functionalities, such as operating system interfaces, network programming, data processing, and more. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint, such as querying system information, modifying files or registry keys, or running other applications.Reference:

Run Python Commands and Scripts

Python Standard Library

Question 8

Question Type: MultipleChoice

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

Options:

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

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.

Initiate a Live Terminal Session

Manage Processes

Manage Files

Run Operating System Commands

Run Python Commands and Scripts

Question 9

Question Type: MultipleChoice

When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

Options:

A- The agent technical support file.

B- The prevention archive from the alert.

C- The distribution id of the agent.

D- A list of all the current exceptions applied to the agent.

E- The unique agent id.

Answer:

A, B

Explanation:

When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:

The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.

The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.

The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:

The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.

A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not

essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.

The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.

Generate and Download the Agent Technical Support File

Generate and Download the Prevention Archive

Cortex XDR Agent Administrator Guide: Agent Distribution ID

Cortex XDR Agent Administrator Guide: Exception Security Profiles

[Cortex XDR Agent Administrator Guide: Unique Agent ID]

Question 10

Question Type: **MultipleChoice**

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

Options:

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.

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.Reference: Cortex XDR 3: Responding to Attacks1, Action Center2