Free Questions for PCDRA by dumpshq

Shared by Knapp on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Create an alert-starring configuration.

B- Create an Incident-starring configuration.

C- Manually star an alert.

D- Manually star an Incident.

Answer:

C, D

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.

Star Security Events

Create an Alert Starring Configuration

Create an Incident Starring Configuration

Question 2

Question Type: **MultipleChoice**

Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

Options:

A- NetBIOS over TCP

B- WebSocket

C- UDP and a random port

D- TCP, over port 80

Answer:

B

Explanation:

Live Terminal uses theWebSocketprotocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic.Reference:

Initiate a Live Terminal Session

WebSocket

Question 3

Question Type: MultipleChoice

Which of the following is NOT a precanned script provided by Palo Alto Networks?

Options:

A- delete_file

B- quarantine_file

C- process_kill_name

D- list_directories

Answer:

D

Explanation:

Palo Alto Networks provides a set of precanned scripts that you can use to perform various actions on your endpoints, such as deleting files, killing processes, or quarantining malware. The precanned scripts are written in Python and are available in the Agent Script

Library in the Cortex XDR console. You can use the precanned scripts as they are, or you can customize them to suit your needs. The precanned scripts are:

delete_file: Deletes a specific file from a local or removable drive.

quarantine_file: Moves a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

process_kill_name: Kills a process by its name on the endpoint.

process_kill_pid: Kills a process by its process ID (PID) on the endpoint.

process_kill_tree: Kills a process and all its child processes by its name on the endpoint.

process_kill_tree_pid: Kills a process and all its child processes by its PID on the endpoint.

process_list: Lists all the processes running on the endpoint, along with their names, PIDs, and command lines.

process_list_tree: Lists all the processes running on the endpoint, along with their names, PIDs, command lines, and parent processes.

process_start: Starts a process on the endpoint by its name or path.

registry_delete_key: Deletes a registry key and all its subkeys and values from the Windows registry.

registry_delete_value: Deletes a registry value from the Windows registry.

registry_list_key: Lists all the subkeys and values under a registry key in the Windows registry.

registry_list_value: Lists the value and data of a registry value in the Windows registry.

registry_set_value: Sets the value and data of a registry value in the Windows registry.

The script list_directories isnota precanned script provided by Palo Alto Networks. It is a custom script that you can write yourself using Python commands.

Run Scripts on an Endpoint

Agent Script Library

Precanned Scripts

Question 4

Question Type: **MultipleChoice**

Which module provides the best visibility to view vulnerabilities?

Options:

A- Live Terminal module

B- Device Control Violations module

C- Host Insights module

D- Forensics module

Answer:

C

Explanation:

TheHost Insights moduleprovides the best visibility to view vulnerabilities on your endpoints. The Host Insights module is an add-on feature for Cortex XDR that combines vulnerability management, application and system visibility, and a Search and Destroy feature to help you identify and contain threats. The vulnerability management feature allows you to scan your Windows endpoints for known vulnerabilities and missing patches, and view the results in the Cortex XDR console. You can also filter and sort the vulnerabilities by severity, CVSS score, CVE ID, or patch availability. The Host Insights module helps you reduce your exposure to threats and improve your security posture.Reference:

Host Insights

Vulnerability Management

Question 5

Question Type: MultipleChoice

Which profiles can the user use to configure malware protection in the Cortex XDR console?

Options:

A- Malware Protection profile

B- Malware profile

C- Malware Detection profile

D- Anti-Malware profile

Answer:

A

Explanation:

The user can use theMalware Protection profileto configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints.Reference:

Malware Protection Profile

Question 6

Question Type: MultipleChoice

Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

Options:

A- exception profiles that apply to specific endpoints

B- agent exception profiles that apply to specific endpoints

C- global exception profiles that apply to all endpoints

D- role-based profiles that apply to specific endpoints

Answer:

B, C

Explanation:

Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives.Reference:

Exception Security Profiles

Create an Agent Exception Profile

Create a Global Exception Profile

Question 7

Question Type: MultipleChoice

After scan, how does file quarantine function work on an endpoint?

Options:

A- Quarantine takes ownership of the files and folders and prevents execution through access control.

B- Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.

C- Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

D- Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

Answer:

C

Explanation:

Quarantine is a feature of Cortex XDR that allows you to isolate a malicious file from its original location and prevent it from being executed. Quarantine works by moving the file to a protected folder on the endpoint and changing its permissions and attributes. Quarantine can be applied to files detected by periodic scans or by behavioral threat protection (BTP) rules. Quarantine is only supported for portable executable (PE) and dynamic link library (DLL) files. Quarantine does not affect the network connectivity or the communication of the endpoint with Cortex XDR.Reference:

Quarantine Malicious Files

Manage Quarantined Files

Question 8

Question Type: MultipleChoice

Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?

Options:

A- Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.

B- Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.

C- Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.

D- Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

Answer:

D

Explanation:

Cortex XDR Analytics is a cloud-based service that uses machine learning and artificial intelligence to detect and prevent network attacks. Cortex XDR Analytics can interfere with the attack pattern as soon as it is observed on the endpoint by applying protection policies that block malicious processes, files, or network connections. This way, Cortex XDR Analytics can stop the attack before it causes any damage or compromises the system.Reference:

[Cortex XDR Analytics Overview]

[Cortex XDR Analytics Protection Policies]

Question 9

Question Type: MultipleChoice

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?

Options:

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

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.

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 10

Question Type: **MultipleChoice**

Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

Options:

A- Hash Verdict Determination

B- Behavioral Threat Protection

C- Restriction Policy

D- Child Process Protection

Answer:

A

Explanation:

The first protection module that is checked in the Cortex XDR Windows agent malware protection flow is the Hash Verdict Determination. This module compares the hash of the executable file that is about to run on the endpoint with a list of known malicious hashes stored in the Cortex XDR cloud. If the hash matches a malicious hash, the agent blocks the execution and generates an alert.If the hash does not match a malicious hash, the agent proceeds to the next protection module, which is the Restriction Policy1.

The Hash Verdict Determination module is the first line of defense against malware, as it can quickly and efficiently prevent known threats from running on the endpoint. However, this module cannot protect against unknown or zero-day threats, which have no known hash signature.Therefore, the Cortex XDR agent relies on other protection modules, such as Behavioral Threat Protection, Child Process Protection, and Exploit Protection, to detect and block malicious behaviors and exploits that may occur during the execution of the file1.

Palo Alto Networks Cortex XDR Documentation, File Analysis and Protection Flow

Question 11

Question Type: MultipleChoice

Which of the following represents the correct relation of alerts to incidents?

Options:

A- Only alerts with the same host are grouped together into one Incident in a given time frame.

B- Alerts that occur within a three-hour time frame are grouped together into one Incident.

C- Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D- Every alert creates a new Incident.

Answer:

C

Explanation:

The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts,

such as the alert source, type, and time period, to determine if they belong to the same causality chain.By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details1.

Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack.

Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.

Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.

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

Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2

Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

Question 12

Question Type: MultipleChoice

Which of the following is an example of a successful exploit?

Options:

A- connecting unknown media to an endpoint that copied malware due to Autorun.

B- a user executing code which takes advantage of a vulnerability on a local service.

C- identifying vulnerable services on a server.

D- executing a process executable for well-known and signed software.

Answer:

B

Explanation:

A successful exploit is a piece of software or code that takes advantage of a vulnerability and executes malicious actions on the target system. A vulnerability is a weakness or flaw in a software or hardware component that can be exploited by an attacker. A successful

exploit is one that achieves its intended goal, such as gaining unauthorized access, executing arbitrary code, escalating privileges, or compromising data.

In the given options, only B is an example of a successful exploit, because it involves a user executing code that exploits a vulnerability on a local service, such as a web server, a database, or a network protocol. This could allow the attacker to gain control over the service, access sensitive information, or perform other malicious actions.

Option A is not a successful exploit, because it involves connecting unknown media to an endpoint that copied malware due to Autorun. Autorun is a feature that automatically runs a program or script when a removable media, such as a USB drive, is inserted into a computer. This feature can be abused by malware authors to spread their malicious code, but it is not an exploit in itself. The malware still needs to exploit a vulnerability on the endpoint to execute its payload and cause damage.

Option C is not a successful exploit, because it involves identifying vulnerable services on a server. This is a step in the reconnaissance phase of an attack, where the attacker scans the target system for potential vulnerabilities that can be exploited. However, this does not mean that the attacker has successfully exploited any of the vulnerabilities, or that the vulnerabilities are even exploitable.

Option D is not a successful exploit, because it involves executing a process executable for well-known and signed software. This is a legitimate action that does not exploit any vulnerability or cause any harm. Well-known and signed software are programs that are widely used and trusted, and have a digital signature that verifies their authenticity and integrity. Executing such software does not pose a security risk, unless the software itself is malicious or compromised.

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

What Is an Exploit? Definition, Types, and Prevention Measures(https://heimdalsecurity.com/blog/what-is-an-exploit/)

Exploit Definition & Meaning - Merriam-Webster(https://www.merriam-webster.com/dictionary/exploit)