Free Questions for CCFA-200 by braindumpscollection

Shared by French on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When creating a custom IOA for a specific domain, which syntax would be best for detecting or preventing on all subdomains as well?

Options:

A- *\.baddomain\.xyz|baddomain\. xyz

B- *baddomain\. xyz|baddomain\. xyz. *

C- Custom IOA rules cannot be created for domains

D- **baddomain\. xyz|baddomain\. xyz**

Answer:

A

Explanation:

The syntax that would be best for detecting or preventing on all subdomains as well is *.baddomain.xyz|baddomain. xyz. This syntax will match any domain that ends with .baddomain.xyz or is exactly baddomain.xyz. The * wildcard will match any characters before the dot, and the | operator will match either side of the expression.This syntax can be used in a Custom IOC or a Custom IOA rule to detect or

prevent network connections to malicious domains1.

Question 2

Question Type: MultipleChoice

Which of the following uses Regex to create a detection or take a preventative action?

Options:

A- Custom IOC

B- Machine Learning Exclusion

C- Custom IOA

D- Sensor Visibility Exclusion

Answer:

C

Explanation:

The option that uses regex to create a detection or take a preventative action is Custom IOA. A Custom IOA (indicator of attack) allows you to define custom rules for detecting or preventing suspicious behavior based on process execution, file write, network connection, or registry events.You can use regex syntax to create a Custom IOA rule that matches the event data that you want to monitor or block1.

Question 3

Question Type: MultipleChoice

What would be the most appropriate action to take if you wanted to prevent a folder from being uploaded to the cloud without disabling uploads globally?

Options:

A- A Machine Learning exclusion

B- A Sensor Visibility exclusion

C- An IOA exclusion

D- A Custom IOC entry

Answer:

D

Explanation:

The most appropriate action to take if you wanted to prevent a folder from being uploaded to the cloud without disabling uploads globally is to create a Custom IOC entry. A Custom IOC (indicator of compromise) entry allows you to define custom rules for detecting or preventing malicious activity based on file hashes, file paths, IP addresses, or domains.You can use regex (regular expression) syntax to create a Custom IOC entry that matches the folder path that you want to block from being uploaded to the cloud1.

Question 4

Question Type: MultipleChoice

When the Notify End Users policy setting is turned on, which of the following is TRUE?

Options:

A- End users will not be notified as we would not want to notify a malicious actor of a detection. This setting does not exist

B- End users will be immediately notified via a pop-up that their machine is in-network isolation

C- End-users receive a pop-up notification when a prevention action occurs

D- End users will receive a pop-up allowing them to confirm or refuse a pending quarantine

Answer:

C

Explanation:

When the Notify End Users policy setting is turned on, end-users receive a pop-up notification when a prevention action occurs. This setting allows you to inform the end-users that the Falcon sensor has blocked or quarantined a malicious item on their system.The notification will also provide the name and path of the item, the reason for the prevention, and a link to contact support if needed1.

Question 5

Question Type: MultipleChoice

When creating a Host Group for all Workstations in an environment, what is the best method to ensure all workstation hosts are added to the group?

Options:

A- Create a Dynamic Group with Type=Workstation Assignment

B- Create a Dynamic Group and Import All Workstations

C- Create a Static Group and Import all Workstations

D- Create a Static Group with Type=Workstation Assignment

Answer:

A

Explanation:

The best method to ensure all workstation hosts are added to the group is to create a Dynamic Group with Type=Workstation Assignment. A Dynamic Group is a group that automatically updates its membership based on certain criteria or filters. A Type=Workstation Assignment filter will match all hosts that have the workstation type assigned in their Active Directory domain.This way, any new or existing workstation hosts will be added to the group without manual intervention1.

Question 6

Question Type: MultipleChoice

Which is a filter within the Host setup and management > Host management page?

Options:

A- User name

B- OU

C- BIOS Version

D- Locality

Answer:

B

Explanation:

OU (organizational unit) is a filter within the Host setup and management > Host management page. The Host management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions.You can also filter by OU, which is a logical grouping of hosts based on their Active Directory domain structure1.

Question 7

Question Type: MultipleChoice

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?

Options:

A- SSL inspection should be configured to occur on all Falcon traffic

B- Some network configurations, such as deep packet inspection, interfere with certificate validation

C- HTTPS interception should be enabled to proceed with certificate validation

D- Common sources of interference with certificate pinning include protocol race conditions and resource contention

Answer:

B

Explanation:

The statement that some network configurations, such as deep packet inspection, interfere with certificate validation is true concerning Falcon sensor certificate validation. The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks, which

means that it verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor.Some network configurations, such as deep packet inspection, SSL inspection, or HTTPS interception, may attempt to modify or replace the server certificate, which will cause the sensor to reject the connection and generate an error3.

Question 8

Question Type: MultipleChoice

On a Windows host, what is the best command to determine if the sensor is currently running?

Options:

A- sc query csagent

B- netstat -a

C- This cannot be accomplished with a command

D- ping falcon.crowdstrike.com

Answer:

A

Explanation:

On a Windows host, the best command to determine if the sensor is currently running is sc query csagent. This command will show the status of the csagent service, which is responsible for running the sensor on Windows systems. The output of this command will indicate if the service is running, stopped, or paused.If the service is running, the sensor is also running3.

Question 9

Question Type: MultipleChoice

How does the Unique Hosts Connecting to Countries Map help an administrator?

Options:

A- It highlights countries with known malware

B- It helps visualize global network communication

C- It identifies connections containing threats

D- It displays intrusions from foreign countries

Answer:

B

Explanation:

The Unique Hosts Connecting to Countries Map helps an administrator to visualize global network communication. The map shows the number of unique hosts in your environment that have established network connections to different countries in the past 24 hours.You can use this map to identify unusual or suspicious network activity, such as connections to high-risk countries or regions, or connections from hosts that are not expected to communicate with external entities2.

Question 10

Question Type: MultipleChoice

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase. What settings do you choose?

Options:

A- Detection slider: Extra Aggressive
Prevention slider: Cautious

B- Detection slider: Moderate
Prevention slider: Disabled

C- Detection slider: Cautious
Prevention slider: Cautious

D- Detection slider: Disabled
Prevention slider: Disabled

Answer:

C

Explanation:

The best settings to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase are Cautious for both Detection and Prevention sliders. This setting will enable the sensor to detect and prevent only high-confidence malicious events, while allowing low-confidence events to run without interference.This setting will also generate less noise and false positives than higher settings, such as Moderate or Extra Aggressive1.

Question 11

Question Type: MultipleChoice

Which is the correct order for manually installing a Falcon Package on a macOS system?

Options:

A- Install the Falcon package, then register the Falcon Sensor via the registration package

B- Install the Falcon package, then register the Falcon Sensor via command line

C- Register the Falcon Sensor via command line, then install the Falcon package

D- Register the Falcon Sensor via the registration package, then install the Falcon package

Answer:

B

Explanation:

The correct order for manually installing a Falcon Package on a macOS system is to install the Falcon package, then register the Falcon Sensor via command line. The Falcon package contains the sensor binary and the kernel extension, while the registration package contains the customer ID and the sensor group ID.The registration package is not required for macOS systems, as the registration information can be provided via command line after installing the Falcon package1.

Question 12

Question Type: MultipleChoice

Which of the following is NOT a way to determine the sensor version installed on a specific endpoint?

Options:

A- Use the Sensor Report to filter to the specific endpoint

B- Use the Investigate > Host Search to filter to the specific endpoint

C- Use Host Management to select the desired endpoint. The agent version will be listed in the columns and details

D- From a command line, run the sc query csagent -version command

Answer:

D

Explanation:

From a command line, running the sc query csagent -version command is not a way to determine the sensor version installed on a specific endpoint. This command will only show the status of the csagent service, not the sensor version. The other options are valid ways to determine the sensor version installed on a specific endpoint using Falcon UI or API.You can use the Sensor Report, the Host

Search, or the Host Management features to filter, search, or select the desired endpoint and view the sensor version information12.