Free Questions for CCFA-200 by certscare

Shared by Drake on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What best describes what happens to detections in the console after clicking "Enable Detections" for a host which previously had its detections disabled?

Options:

A- Enables custom detections for the host

B- New detections will start appearing in the console, and all retroactive stored detections will be restored to the console for that host

C- New detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host

D- Preventions will be enabled for the host

Answer:

C

Explanation:

The option that best describes what happens to detections in the console after clicking "Enable Detections" for a host which previously had its detections disabled is that new detections will start appearing in the console immediately. Previous detections will not be restored

to the console for that host. The "Enable Detections" feature allows you to enable or disable the detection and prevention capabilities of the Falcon sensor on a specific host. When you disable detections for a host, the sensor will stop sending any detection or prevention events to the Falcon console, and any existing events for that host will be removed from the console.When you enable detections for a host, the sensor will resume sending any new detection or prevention events to the Falcon console, but any previous events for that host will not be restored to the console1.

Question 2

Question Type: MultipleChoice

Which of the following pages provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System?

Options:

A- Support and resources

B- Activity Overview

C- Hosts Overview

D- Sensor Health

Answer:

D

Explanation:

The page that provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System is Sensor Health. The Sensor Health page allows you to view and monitor the health and status of all sensors in your environment. You can use this page to identify any sensors that have issues or errors, such as RFM, which is a mode that limits the sensor's functionality due to license expiration, network connectivity loss, or certificate validation failure.You can filter the sensors by operating system, sensor version, last seen date, health events, detections, and preventions3.

Question 3

Question Type: MultipleChoice

How many days will an inactive host remain visible within the Host Management or Trash pages?

Options:

A- 45 days

B- 15 days

C- 90 days

D- 120 days

Answer:

C

Explanation:

An inactive host will remain visible within the Host Management or Trash pages for 90 days. An inactive host is a host that has not communicated with the Falcon platform for more than seven days. An inactive host will be moved from the Host Management page to the Trash page after seven days of inactivity. An inactive host will remain in the Trash page for 90 days before being permanently deleted from the Falcon platform.You can restore an inactive host from the Trash page if it becomes active again within 90 days1.

Question 4

Question Type: MultipleChoice

Which of the following scenarios best describes when you would add IP addresses to the containment policy?

Options:

A- You want to automate the Network Containment process based on the IP address of a host

B- Your organization has additional IP addresses that need to be able to access the Falcon console

C- A new group of analysts need to be able to place hosts under Network Containment

D- Your organization has resources that need to be accessible when hosts are network contained

Answer:

D

Explanation:

The scenario that best describes when you would add IP addresses to the containment policy is that your organization has resources that need to be accessible when hosts are network contained. As explained in the previous question, adding IP addresses to the containment policy allows you to create an allowlist of trusted IP addresses that can communicate with your contained hosts.This can be useful when you need to isolate a host from the network due to a potential compromise or investigation, but still want to allow it to access certain resources or services that are essential for your organization's operations or security2.

Question 5

Question Type: MultipleChoice

You have a new patch server that should be reachable while hosts in your environment are network contained. The server's IP address is static and does not change. Which of the following is the best approach to updating the Containment Policy to allow this?

Options:

A- Add an allowlist entry for the individual server's MAC address

B- Add an allowlist entry containing the host group that the server belongs to

C- Add an allowlist entry for the individual server's IP address

D- Add an allowlist entry containing CIDR notation for the /24 network the server belongs to

Answer:

C

Explanation:

The best approach to updating the Containment Policy to allow a new patch server that should be reachable while hosts in your environment are network contained is to add an allowlist entry for the individual server's IP address. An allowlist entry allows you to define a list of trusted IP addresses that can communicate with your contained hosts. This way, you can isolate a host from the network while still allowing it to access essential resources or services, such as a patch server.If the server's IP address is static and does not change, adding an individual IP address is more precise and secure than adding a host group or a network range2.

Question 6

Question Type: MultipleChoice

A. Enable Behavior-Based Threat Prevention sliders and Advanced Remediation Actions

Options:

B- Enable Malware Protection and Windows Anti-Malware Execution Blocking

C- Enable Next-Gen Antivirus Prevention sliders and 'Quarantine & Security Center Registration

D- Enable Malware Protection and Custom Execution Blocking

Answer:

C

Explanation:

The option that will enable Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration" is to enable Malware Protection and Windows Anti-Malware Execution Blocking. Malware Protection is a feature that enables the Next-Gen Antivirus Prevention sliders, which allow you to adjust the level of sensitivity and aggressiveness of the Falcon sensor's machine learning engine, which uses artificial intelligence to identify and stop unknown threats.Windows Anti-Malware Execution Blocking is a feature that enables the "Quarantine & Security Center Registration" setting, which allows you to quarantine malicious files and register them in the Windows Security Center1.