Free Questions for CCFA-200

Shared by Snyder on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Once an exclusion is saved, what can be edited in the future?

Options:

A- All parts of the exclusion can be changed

B- Only the selected groups and hosts to which the exclusion is applied can be changed

C- Only the options to 'Detect/Block' and/or 'File Extraction' can be changed

D- The exclusion pattern cannot be changed

Answer:

A

Explanation:

Once an exclusion is saved, all parts of the exclusion can be changed in the future. The administrator can edit an existing exclusion by selecting it from the Exclusions page and modifying any of its fields, such as pattern, type, option, group or host. The other options are either incorrect or not true of editing exclusions. Reference:CrowdStrike Falcon User Guide, page 37.

Question 2

Question Type: MultipleChoice

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from uninstalling or upgrading the sensor, which settings in the Sensor Update Policy would meet this criteria?

Options:

A- Sensor version set to N-1 and Bulk maintenance mode is turned on

B- Sensor version fixed and Uninstall and maintenance protection turned on

C- Sensor version updates off and Uninstall and maintenance protection turned off

D- Sensor version set to N-2 and Bulk maintenance mode is turned on

Answer:

B

Explanation:

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from uninstalling or upgrading the sensor, the administrator should set the Sensor version to fixed and turn on the Uninstall and maintenance protection setting in the Sensor Update Policy. This will allow the administrator to specify which sensor version will be used by the hosts using this policy, and also require a maintenance token to uninstall or upgrade the sensor. The other options are either incorrect or not sufficient to meet this criteria. Reference:CrowdStrike Falcon User Guide, page 38.

Question 3

Question Type: MultipleChoice

You are evaluating the most appropriate Prevention Policy Machine Learning slider settings for your environment. In your testing phase, you configure the Detection slider as Aggressive. After running the sensor with this configuration for 1 week of testing, which Audit report should you review to determine the best Machine Learning slider settings for your organization?

Options:

A- Prevention Policy Audit Trail

B- Prevention Policy Debug

C- Prevention Hashes Ignored

D- Machine-Learning Prevention Monitoring

Answer:

D

Explanation:

Audit logs --> Machine-learning prevention monitoring It shows the count of ML expected detections based on the detection levels for a defined time period and the list of files that would be detected on each detection level.

Question 4

Question Type: **MultipleChoice**

What is the maximum number of patterns that can be added when creating a new exclusion?

Options:

A- 10

B- 0

C- 1

D- 5

Answer:

C

Explanation:

The maximum number of patterns that can be added when creating a new exclusion is one. Each exclusion can only have one pattern, which can be a file path, a hash, a command line or a user name. The other options are either incorrect or not related to creating exclusions. Reference:CrowdStrike Falcon User Guide, page 37.

Question 5

Question Type: MultipleChoice

Which role will allow someone to manage quarantine files?

Options:

A- Falcon Security Lead

B- Detections Exceptions Manager

C- Falcon Analyst -- Read Only

D- Endpoint Manager

Answer:

A

Explanation:

The role that will allow someone to manage quarantine files is Falcon Security Lead. This role allows users to view and manage quarantined files, as well as release them from quarantine or download them for further analysis. The other roles do not have this capability. Reference:CrowdStrike Falcon User Guide, page 19.

Question 6

Question Type: MultipleChoice

You need to export a list of all deletions for a specific Host Name in the last 24 hours. What is the best way to do this?

Options:

A- Go to Host Management in the Host page. Select the host and use the Export Detections button

B- Utilize the Detection Resolution Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the 'Detection Resolution History' section

C- In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results

D- Utilize the Detection Activity Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the 'Detections by Host' section

Answer:

C

Explanation:

The best way to export a list of all deletions for a specific Host Name in the last 24 hours is to go to the Investigate module, access the Detection Activity page, use the filters to focus on the appropriate hostname and time, then export the results. This will allow you to download a CSV file that contains information about all the detections that were deleted for that host in that time period. The other options are either incorrect or not related to exporting deletions. Reference:CrowdStrike Falcon User Guide, page 49.

Question 7

Question Type: MultipleChoice

Which of the following is a valid step when troubleshooting sensor installation failure?

Options:

A- Confirm all required services are running on the system

B- Enable the Windows firewall

C- Disable SSL and TLS on the host

D- Delete any available application crash log files

Answer:

A

Explanation:

A valid step when troubleshooting sensor installation failure is to confirm all required services are running on the system. This can help identify if there are any issues with the sensor service, the Windows Management Instrumentation service, or the Windows Remote Management service, which are required for the sensor to function properly. The other options are either incorrect or not helpful for troubleshooting sensor installation failure. Reference:CrowdStrike Falcon User Guide, page 29.

Question 8

Question Type: MultipleChoice

What is the name for the unique host identifier in Falcon assigned to each sensor during sensor installation?

Options:

A- Endpoint ID (EID)

B- Agent ID (AID)

C- Security ID (SID)

D- Computer ID (CID)

Answer:

B

Explanation:

The name for the unique host identifier in Falcon assigned to each sensor during sensor installation is Agent ID (AID). The AID is a 32-character hexadecimal string that uniquely identifies each sensor and host in the Falcon platform. The other options are either incorrect or not related to the sensor identifier. Reference:CrowdStrike Falcon User Guide, page 28.

Question 9

Question Type: MultipleChoice

Where in the Falcon console can information about supported operating system versions be found?

Options:

A- Configuration module

B- Intelligence module

C- Support module

D- Discover module

Answer:

C

Explanation:

Information about supported operating system versions can be found in the Support module in the Falcon console. This module provides access to various support resources, such as documentation, downloads, FAQs, release notes and system status. One of the documents available in this module is the CrowdStrike Sensor Compatibility List, which lists the supported operating system versions for each sensor type and platform. The other options are either incorrect or not related to finding information about supported operating system versions. Reference:CrowdStrike Falcon User Guide, page 26.

Question 10

Question Type: MultipleChoice

How can a Falcon Administrator configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity?

Options:

A- By ensuring each user has set the 'pop-ups allowed' in their User Profile configuration page

B- By enabling 'Upload quarantined files' in the General Settings configuration page

C- By turning on the 'Notify End Users' setting at the top of the Prevention policy details configuration page

D- By selecting 'Enable pop-up messages' from the User configuration page

Answer:

C

Explanation:

A Falcon Administrator can configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity by turning on the "Notify End Users" setting at the top of the Prevention policy details configuration page. This setting allows users to enable or disable end user notifications for prevention actions taken by Falcon on Windows hosts. The other options are either incorrect or not related to configuring pop-up messages. Reference:CrowdStrike Falcon User Guide, page 36.

Question 11

Question Type: MultipleChoice

When uninstalling a sensor, which of the following is required if the 'Uninstall and maintenance protection' setting is enabled within the Sensor Update Policies?

Options:

A- Maintenance token

B- Customer ID (CID)

C- Bulk update key

D- Agent ID (AID)

Answer:

A

Explanation:

When uninstalling a sensor, a maintenance token is required if the 'Uninstall and maintenance protection' setting is enabled within the Sensor Update Policies. This setting prevents unauthorized or accidental uninstallation of sensors by requiring a token that can be generated from the Falcon console. The other options are either incorrect or not related to uninstalling a sensor. Reference:CrowdStrike Falcon User Guide, page 29.

Question 12

Question Type: MultipleChoice

What is the purpose of precedence with respect to the Sensor Update policy?

Options:

A- Precedence applies to the Prevention policy and not to the Sensor Update policy

B- Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)

C- Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)

D- Precedence ensures that conflicting policy settings are not set in the same policy

Answer:

B

Explanation:

The purpose of precedence with respect to the Sensor Update policy is that hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number). This means that if a host belongs to more than one group that has different Sensor Update policies assigned, it will use the policy that has the highest precedence (lowest number) among them. The other options

are either incorrect or not related to precedence. Reference:CrowdStrike Falcon User Guide, page 38.