Free Questions for CCFA-200 by certsdeals

Shared by Fox on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What can exclusions be applied to?

Options:

A- Individual hosts selected by the administrator

B- Either all hosts or specified groups

C- Only the default host group

D- Only the groups selected by the administrator

Answer:

B

Explanation:

The option that describes what exclusions can be applied to is that exclusions can be applied to either all hosts or specified groups. An exclusion is a rule that defines what files, folders, processes, IP addresses, or domains should be excluded from detection or prevention by the Falcon sensor. You can create and manage exclusions in the Exclusions page in the Falcon console. You can apply exclusions to

either all hosts in your environment or to specific host groups that you select. You cannot apply exclusions to individual hosts selected by the administrator.

Question 2

Question Type: MultipleChoice

You need to have the ability to monitor suspicious VBA macros. Which Sensor Visibility setting should be turned on within the Prevention policy settings?

Options:

A- Script-based Execution Monitoring

B- Interpreter-Only

C- Additional User Mode Data

D- Engine (Full Visibility)

Answer:

A

Explanation:

Turn on the Script-Based Execution Monitoring prevention policy setting to enable the 'Falcon sensor to monitor the contents of scripts and shells that are popular mechanisms for executing malicious code on hosts. This setting does not kill or block scripts.'

Scripting languages:

Excel 4.0 macros

JScript

VBA Macros

VBScript

The Sensor Visibility setting that should be turned on within the Prevention policy settings to monitor suspicious VBA macros is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems. The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash. VBA (Visual Basic for Applications) is a scripting language that can be embedded in Microsoft Office documents, such as Word or Excel. VBA macros can be used to automate tasks or perform actions within the documents, but they can also be abused by attackers to deliver malware or execute malicious code. Script-based Execution Monitoring can help detect and prevent such attacks by monitoring the contents of VBA macros for execution of malicious content.

Question 3

Question Type: MultipleChoice

What is the purpose of the Machine-Learning Prevention Monitoring Report?

Options:

A- It is designed to give an administrator a quick overview of machine-learning aggressiveness settings as well as the numbers of items actually quarantined

B- It is the dashboard used by an analyst to view all items quarantined and to release any items deemed non-malicious

C- It is the dashboard used to see machine-learning preventions, and it is used to identify spikes in activity and possible targeted attacks

D- It is designed to show malware that would have been blocked in your environment based on different Machine-Learning Prevention settings

Answer:

D

Explanation:

Machine-Learning Prevention Monitoring dashboard: Use this dashboard to view malware that would have been blocked in your environment over the selected timeframe based on different Machine Learning Prevention settings (Cautious, Moderate, Aggressive or Extra Aggressive).

Question 4

Question Type: MultipleChoice

The Falcon Administrator has created a new prevention policy to apply to the "Servers" group; however, when applying the new prevention policy this group is not appearing in the list of available groups. What is the most likely issue?

Options:

A- The new prevention policy should be enabled first

B- The 'Servers' group already has a policy applied to it

C- The 'Servers' group must be disabled first

D- Host type was not defined correctly within the prevention policy

Answer:

B

Explanation:

The most likely issue for not being able to apply a new prevention policy to the "Servers" group is that the "Servers" group already has a policy applied to it. A prevention policy is a policy that defines the prevention capabilities and settings for the Falcon sensor on a host. You can create and assign custom prevention policies to different hosts or groups in your environment. However, you can only assign one prevention policy per host or group at a time.If a host or group already has a prevention policy applied to it, you cannot apply another prevention policy to it unless you remove or replace the existing one2.

Question 5

Question Type: MultipleChoice

Which of the following prevention policy settings monitors contents of scripts and shells for execution of malicious content on compatible operating systems?

Options:

A- Script-based Execution Monitoring

B- FileSystem Visibility

C- Engine (Full Visibility)

D- Suspicious Scripts and Commands

Answer:

A

Explanation:

The prevention policy setting that monitors contents of scripts and shells for execution of malicious content on compatible operating systems is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems. The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash.You can enable or disable Script-based Execution Monitoring in the Prevention Policy for Windows hosts1.

Question 6

Question Type: MultipleChoice

What best describes the relationship between Sensor Update policies and Operating Systems?

Options:

A- Windows and Mac share Sensor Update policies. Linux requires its own set of polices based on the different kernel versions

B- Sensor Update polices are not Operating System specific. One policy can be applied to all Operating Systems

C- Windows has its own Sensor Update polices. But Mac and Linux share Sensor Update policies

D- A Sensor Update policy must be configured for each Operating System (Windows, Mac, Linux)

Answer:

D

Explanation:

The option that describes the relationship between Sensor Update policies and Operating Systems is that a Sensor Update policy must be configured for each Operating System (Windows, Mac, Linux). This option is essentially a repetition of question 141 and its answer. Sensor Update policies are specific to each operating system type, as different operating systems have different sensor versions, features, and requirements.Therefore, you need to create and assign separate Sensor Update policies for each operating system type in your environment1.

Question 7

Question Type: MultipleChoice

What is the purpose of the Default Sensor Policy?

Options:

A- A mechanism to deploy the oldest supported version of the Falcon Sensor.

B- Tests the sensor configuration settings before deployment.

C- Used to reset all sensor settings to Default.

D- Acts as a 'catch all' policy if no other Sensor Policies are applied.

Answer:

D

Explanation:

The purpose of the Default Sensor Policy is that it acts as a "catch all" policy if no other Sensor Policies are applied. A Sensor Policy is a policy that defines the detection and prevention settings for the Falcon sensor on a host. You can create and assign custom Sensor Policies to different hosts or groups in your environment. However, if a host is not assigned to a specific Sensor Policy, it will inherit the settings from the Default Sensor Policy. The Default Sensor Policy is a "catch-all" policy that is enabled by default and has the "Malware Protection" feature turned on.You can modify the settings of the Default Sensor Policy, but you cannot delete or disable it1.

Question 8

Question Type: MultipleChoice

Why do Sensor Update policies need to be configured for each OS (Windows, Mac, Linux)?

Options:

A- To bundle the Sensor and Prevention policies together into a deployment package

B- Sensor Update policies are OS dependent

C- To assist with auditing and change management

D- This is false. One policy can be applied to all Operating Systems

Answer:

B

Explanation:

Sensor Update policies need to be configured for each OS (Windows, Mac, Linux) because Sensor Update policies are OS dependent. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. Sensor Update policies are specific to each operating system type, as different operating systems have different sensor versions, features, and requirements.Therefore, you need to create and assign separate Sensor Update policies for each operating system type in your environment1.

Question 9

Question Type: MultipleChoice

Which statement describes what is recommended for the Default Sensor Update policy?

Options:

A- The Default Sensor Update policy should align to an organization's overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible

B- The Default Sensor Update should be configured to always automatically upgrade to the latest sensor version

C- Since the Default Sensor Update policy is pre-configured with recommend settings out of the box, configuration of the Default Sensor Update policy is not required

D- No configuration is required. Once a Custom Sensor Update policy is created the Default Sensor Update policy is disabled

Answer:

A

Explanation:

The statement that describes what is recommended for the Default Sensor Update policy is that the Default Sensor Update policy should align to an organization's overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible. As explained in question 139, the Default Sensor Update policy is a "catch-all" policy that applies to any host that is not assigned to a specific Sensor Update policy. Therefore, it is recommended that the Default Sensor Update policy should align to your organization's overall sensor updating practice, such as how frequently and how quickly you want to update your sensors.It is also recommended that you leverage the Auto N-1 and Auto N-2 configurations, which allow you to automatically update your sensors to the latest or second-latest sensor version without requiring manual intervention1.

Question 10

Question Type: MultipleChoice

What will happen to a host if it is not assigned a Sensor Update policy?

Options:

A- The host will uninstall the Sensor and provide an alert to the installation team

B- The host will automatically update to the newest sensor version and auto-update to future release

C- The host will automatically create a custom Sensor Update policy

D- The host will use the Default Sensor Update policy

Answer:

D

Explanation:

The option that describes what will happen to a host if it is not assigned a Sensor Update policy is that the host will use the Default Sensor Update policy. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. You can create and assign custom Sensor Update policies to different hosts or groups in your environment. However, if a host is not assigned to a specific Sensor Update policy, it will inherit the settings from the Default Sensor Update policy. The Default Sensor Update policy is a "catch-all" policy that is enabled by default and has the "Uninstall and Maintenance Protection" feature turned on.You can modify the settings of the Default Sensor Update policy, but you cannot delete or disable it1.

Question 11

Question Type: MultipleChoice

How can a API client secret be viewed after it has been created?

Options:

A- Within the API management page, API client secrets can be accessed within the 'edit client' functionality

B- The API client secret must be reset or a new client created as the secret cannot be viewed after it has been created

C- The API client secret can be provided by support via direct email request from a Falcon Administrator

D- Selecting 'show secret' within the 3-dot dropdown menu will reveal the secret for the selected api client

Answer:

B

Explanation:

The way an API client secret can be viewed after it has been created is that the API client secret must be reset or a new client created as the secret cannot be viewed after it has been created. As explained in question 137, an API client secret is only displayed once during creation for security reasons. If you lose or forget your API client secret, you cannot view it again in the Falcon console. You have two options to resolve this issue: either reset your API client secret or create a new API client. Resetting your API client secret will generate a new secret for your existing API client, which will invalidate any previous secret.Creating a new API client will generate a new API client ID and secret, which will require you to update any applications or scripts that use the Falcon APIs2.