Free Questions for CCFA-200 by certsinside

Shared by Clemons on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Where should you look to find the history of the successes and failures for any Falcon Fusion workflows?

Options:

A- Workflow Execution log

B- Falcon Ul Audit Trail

C- Workflow Audit log

D- Custom Alert History

Answer:

A

Explanation:

The place where you can find the history of the successes and failures for any Falcon Fusion workflows is the Workflow Execution log. The Workflow Execution log in the Workflow Management option allows you to view the status and results of workflow executions triggered by detection events. You can filter the log by workflow name, status, start and end time, and detection ID. You can also view

the details of each execution, including the actions performed, the output received, and any errors encountered.This log can help you troubleshoot potential failures or issues with your workflows1.

Question 2

Question Type: MultipleChoice

What three things does a workflow condition consist of?

Options:

A- A parameter, an operator, and a value

B- A beginning, a middle, and an end

C- Triggers, actions, and alerts

D- Notifications, alerts, and API's

Answer:

A

Explanation:

A workflow condition consists of a parameter, an operator, and a value. A workflow condition is a rule that defines when a workflow should be triggered based on certain criteria or filters. A parameter is a variable or attribute that can be used to filter or match detection events, such as severity, tactic, or host group. An operator is a symbol or word that specifies how to compare or evaluate the parameter and the value, such as equals, contains, or greater than.A value is a constant or expression that provides the expected or desired result for the parameter, such as high, credential dumping, or default group1.

Question 3

Question Type: MultipleChoice

What information does the API Audit Trail Report provide?

Options:

A- A list of analyst login activity

B- A list of specific changes to prevention policy

C- A list of actions taken via Falcon OAuth2-based APIs

D- A list of newly added hosts

Answer:

C

Explanation:

The information that the API Audit Trail Report provides is a list of actions taken via Falcon OAuth2-based APIs. The API Audit Trail Report allows you to view and audit the activity and usage of the Falcon APIs by different API clients and users in your organization.You can use this report to monitor who accessed what data, when, and how via the Falcon APIs2.

Question 4

Question Type: MultipleChoice

You have been asked to troubleshoot why Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host. Which report can be used to determine if this is an issue with an old prevention policy?

Options:

A- Host Update Status Report

B- Custom Alerting Audit Trail

C- Prevention Policy Debug

D- SBEM Debug Report

Answer:

C

Explanation:

The report that can be used to determine if Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host due to an old prevention policy is Prevention Policy Debug. The Prevention Policy Debug report allows you to view and compare the prevention policy settings applied to each host in your environment.You can use this report to identify any hosts that have outdated or inconsistent prevention policy settings, such as SBEM, which is a feature that monitors and prevents malicious script execution on Windows systems1.

Question 5

Question Type: MultipleChoice

When troubleshooting the Falcon Sensor on Windows, what is the correct parameter to output the log directory to a specified file?

Options:

A- LOG=log.txt

B- \log log.txt

C- C:\CSSensorInstall\LogFiles

D- /log log.txt

Answer:

D

Explanation:

The correct parameter to output the log directory to a specified file when troubleshooting the Falcon Sensor on Windows is /log log.txt. This parameter will create a log file named log.txt in the same folder where you run the sensor installation command.The log file will contain information about the sensor installation process, such as the parameters used, the actions performed, and any errors encountered3.

Question 6

Question Type: MultipleChoice

What should be disabled on firewalls so that the sensor's man-in-the-middle attack protection works properly?

Options:

A- Deep packet inspection

B- Linux Sub-System

C- PowerShell

D- Windows Proxy

Answer:

A

Explanation:

The option that should be disabled on firewalls so that the sensor's man-in-the-middle attack protection works properly is deep packet inspection. Deep packet inspection is a network configuration that inspects and modifies the data packets that pass through a firewall. Deep packet inspection may interfere with the sensor's certificate validation, which is a feature that verifies that the server certificate

presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor.If the certificate validation fails, the sensor will reject the connection and generate an error3.

Question 7

Question Type: MultipleChoice

A Falcon Administrator is trying to use Real-Time Response to start a session with a host that has a sensor installed but they are unable to connect. What is the most likely cause?

Options:

A- The host has a user logged into it

B- The domain controller is preventing the connection

C- They do not have an RTR role assigned to them

D- There is another analyst connected into it

Answer:

C

Explanation:

The most likely cause for not being able to use Real-Time Response to start a session with a host that has a sensor installed is that they do not have an RTR role assigned to them. An RTR (Real Time Response) role is a role that grants access and permissions to use the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. There are three types of RTR roles: Real Time Response -Read-Only Analyst, Real Time Response -Active Responder, and Real Time Response - Administrator.You need to have at least one of these roles assigned to you in order to use Real Time Response2.

Question 8

Question Type: MultipleChoice

Where can you find your company's Customer ID (CID)?

Options:

A- The CID is a secret key used for Falcon communication and is never shared with the customer

B- The CID is only available by calling support

C- The CID is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the

checksum

D- The CID is located at Hosts > Host Management

Answer:

C

Explanation:

The CID (Customer ID) is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the checksum. The CID is a unique identifier for your organization that is required for authenticating your sensor installation and communication with the Falcon cloud. The checksum is a value that verifies the integrity of the sensor download file.You can find your CID and checksum at the top of the Sensor Downloads page1.

Question 9

Question Type: MultipleChoice

Which option best describes the general process Whereinstallation of the Falcon Sensor on MacOS?

Options:

A- Grant the Falcon Package Full Disk Access, install the Falcon package, use falconctl to license the sensor

B- Install the Falcon package passing it the installation token in the command line

C- Install the Falcon package, use falconctl to license the sensor, approve the system extension, grant the sensor Full Disk Access

D- Grant the Falcon Package Full Disk Access, install the Falcon package, load the Falcon Sensor with the command 'falconctl stats'

Answer:

C

Explanation:

The option that best describes the general process for installation of the Falcon Sensor on MacOS is to install the Falcon package, use falconctl to license the sensor, approve the system extension, grant the sensor Full Disk Access. The Falcon package contains the sensor binary and the kernel extension, which can be installed by double-clicking on it or using a command-line tool such as installer. The falconctl tool is a command-line utility that allows you to configure and manage the sensor on MacOS systems. You can use falconctl to license the sensor by providing your Customer ID (CID) and optionally your Sensor Group ID (SGID). After licensing the sensor, you need to approve the system extension in the Security & Privacy settings of your system preferences, which will require a restart.Finally, you need to grant the sensor Full Disk Access in the Privacy settings of your system preferences, which will allow the sensor to monitor and protect your files and folders1.