Free Questions for CCFA-200 by actualtestdumps

Shared by Reyes on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following best describes what the Uninstall and Maintenance Protection setting controls within your Sensor Update Policy?

Options:

A- Prevents automatic updates of the sensor

B- Prevents the sensor from entering Reduced Functionality Mode

C- Prevents modification of sensor update policy

D- Prevents unauthorized uninstallation of the sensor

Answer:

D

Explanation:

The option that best describes what the Uninstall and Maintenance Protection setting controls within your Sensor Update Policy is that it prevents unauthorized uninstallation of the sensor. The Uninstall and Maintenance Protection setting is a feature that adds an extra layer of security to the sensor by requiring a maintenance token to uninstall or update the sensor manually. The maintenance token is a

unique code that can be generated by a Falcon Administrator or a Real Time Response -Administrator in the Falcon console.Without a valid maintenance token, the sensor cannot be uninstalled or updated by anyone, including local administrators or malware2.

Question 2

Question Type: MultipleChoice

After agent installation, an agent opens a permanent___connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated.

Options:

A- SSH

B- TLS

C- HTTP

D- TCP

Answer:

B

Explanation:

After agent installation, an agent opens a permanent TLS connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated. TLS (Transport Layer Security) is a protocol that provides secure and encrypted communication between the agent and the Falcon cloud. Port 443 is the standard port for HTTPS (Hypertext Transfer Protocol Secure) traffic.The agent uses this connection to send and receive data, commands, policies, and updates from the Falcon cloud2.

Question 3

Question Type: MultipleChoice

When a user initiates a sensor installs, where can the logs be found?

Options:

A- %SYSTEMROOT%\Logs

B- %SYSTEMROOT%\Temp

C- %LOCALAPPDATA%\Logs

D- % LOCALAPP D ATA%\Tem p

Answer:

B

Explanation:

When a user initiates a sensor install, the logs can be found in %SYSTEMROOT%\Temp. This folder contains temporary files and folders created by the system or applications, including the sensor installation logs. The sensor installation logs have names that start with CSFalconContainer and end with .log, such as CSFalconContainer-2023-08-31_11-23-21.log.These logs can help you troubleshoot any issues or errors that may occur during the sensor installation process3.

Question 4

Question Type: MultipleChoice

Which of the following tools developed by Crowdstrike is intended to help with removal of the CrowdStrike Windows Falcon Sensor?

Options:

A- CrowdStrikeRemovalTool.exe

B- UninstallTool.exe

C- CSUninstallTool.exe

D- FalconUninstall.exe

Answer:

C

Explanation:

The tool developed by Crowdstrike that is intended to help with removal of the CrowdStrike Windows Falcon Sensor is CSUninstallTool.exe. This tool is a command-line utility that can uninstall the Falcon sensor from a Windows system without requiring user interaction or network connectivity.The tool can also bypass the Uninstall and Maintenance Protection feature if enabled in the Sensor Update Policy2.

Question 5

Question Type: MultipleChoice

Which of the following controls the speed in which your sensors will receive automatic sensor updates?

Options:

A- Maintenance Tokens

B- Sensor Update Policy

C- Sensor Update Throttling

D- Channel File Update Throttling

Answer:

C

Explanation:

The option that controls the speed in which your sensors will receive automatic sensor updates is Sensor Update Throttling. Sensor Update Throttling allows you to limit the number of sensors that can download a new sensor version per hour. This way, you can avoid network congestion or bandwidth issues caused by simultaneous sensor updates.You can configure the Sensor Update Throttling setting in the Sensor Update Policy for each platform1.

Question 6

Question Type: MultipleChoice

After Network Containing a host, your Incident Response team states they are unable to remotely connect to the host. Which of the following would need to be configured to allow remote connections from specified IP's?

Options:

A- Response Policy

B- Containment Policy

C- Maintenance Token

D- IP Allowlist Management

Answer:

D

Explanation:

The option that would need to be configured to allow remote connections from specified IP's after network containing a host is IP Allowlist Management. IP Allowlist Management 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 your incident response team or other authorized parties to remotely connect to the host for investigation or remediation purposes2.

Question 7

Question Type: MultipleChoice

On which page of the Falcon console can one locate the Customer ID (CID)?

Options:

A- Hosts Management

B- API Clients and Keys

C- Sensor Dashboard

D- Sensor Downloads

Answer:

B

Explanation:

The page of the Falcon console where one can locate the Customer ID (CID) is API Clients and Keys. The API Clients and Keys page allows you to create and manage API clients and keys for accessing the Falcon platform programmatically. The Customer ID (CID) is a unique identifier for your organization that is required for authenticating your API requests.You can find your CID at the top of the API Clients and Keys page2.

Question 8

Question Type: MultipleChoice

Which command would tell you if a Falcon Sensor was running on a Windows host?

Options:

A- cswindiag.exe -status

B- netstat.exe -f

C- sc.exe query csagent

D- sc.exe query falcon

Answer:

C

Explanation:

The command that would tell you if a Falcon Sensor was running on a Windows host is sc.exe 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

Which Real Time Response role will allow you to see all analyst session details?

Options:

A- Real Time Response - Read-Only Analyst

B- None of the Real Time Response roles allows this

C- Real Time Response -Active Responder

D- Real Time Response -Administrator

Answer:

D

Explanation:

The Real Time Response role that will allow you to see all analyst session details is Real Time Response -Administrator. A Real Time Response -Administrator is a role that has full access and control over the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. A Real Time Response -Administrator can view all analyst session details, such as session ID, host name, start and end time, commands executed, and output received.A Real Time Response -Administrator can also create, modify, delete, and assign scripts and commands to other analysts2.

Question 10

Question Type: MultipleChoice

What statement is TRUE about managing a user's role?

Options:

A- The Administrator cannot re-use the account email for a new account

B- You must have Falcon MFA enabled first

C- You must be a Falcon Security Lead

D- You must be a Falcon Administrator

Answer:

D

Explanation:

The statement that is true about managing a user's role is that you must be a Falcon Administrator. A Falcon Administrator is a role that has full access and control over all features and functions in Falcon, including user management. A Falcon Administrator can create, modify, delete, and assign roles to other users in Falcon.A Falcon Administrator can also re-use the account email for a new account, enable Falcon MFA (multi-factor authentication), and assign other roles such as Falcon Security Lead or Falcon Investigator2.