CCFA-200$^{Q\&As}$

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

QUESTION 1

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

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\\'

Correct Answer: C

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 and 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. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?

A. Sensor Report

B. Machine Learning Prevention Monitoring

C. Falcon UI Audit Trail

D. Machine Learning Debug

Correct Answer: B

The Machine Learning Prevention Monitoring report in the Prevention Policy Management option allows you to monitor the impact of machine learning (ML) prevention settings on your environment. You can view the number of ML detections and preventions by severity, policy, and host group. You can also drill down into specific events and hosts to see more details. This report can help you determine the appropriate ML levels to set in a prevention policy based on your risk tolerance and security posture1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 3

What best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page?

A. The detections for the host are removed from the console immediately and no new detections will display in the console going forward

B. You cannot disable detections for a host

C. Existing detections for the host remain, but no new detections will display in the console going forward

D. Preventions will be disabled for the host

Correct Answer: A

The option that best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page is that the detections for the host are removed from the console immediately and no new detections will display in the console going forward. The "Disable 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. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 4

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

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

Correct Answer: D

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.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 5

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

A. Endpoint ID (EID)

B. Agent ID (AID)

C. Security ID (SID)

D. Computer ID (CID)

Correct Answer: B

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.