CCFA-200Q&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.pass4itsure.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 of the following Machine Learning (ML) sliders will only detect or prevent high confidence malicious items?

A. Aggressive

B. Cautious

C. Minimal

D. Moderate

Correct Answer: B

The Machine Learning (ML) slider that will only detect or prevent high confidence malicious items is Cautious. The ML slider allows you to adjust the level of sensitivity and aggressiveness of the Falcon sensor\\'s ML engine, which uses artificial intelligence to identify and stop unknown threats. The Cautious setting will enable the sensor to detect and prevent only high-confidence malicious events, while allowing low- confidence events to run without interference. This setting will also generate less noise and false positives than higher settings, such as Moderate or Extra Aggressive. References: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

Which of the follow should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax?

A. Sensor Visibility Exclusion

B. Machine Learning Exclusions

C. IOC Exclusions

D. IOA Exclusions

Correct Answer: D

The option that should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax is IOA Exclusions. An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. However, using IOA exclusions may reduce the visibility and protection of the Falcon sensor, as it may allow malicious activity to bypass the sensor\\'s detection and prevention capabilities. Therefore, you should use IOA exclusions with extreme caution and only when necessary2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 3

Which is the correct order for manually installing a Falcon Package on a macOS system?

A. Install the Falcon package, then register the Falcon Sensor via the registration package

B. Install the Falcon package, then register the Falcon Sensor via command line

C. Register the Falcon Sensor via command line, then install the Falcon package

D. Register the Falcon Sensor via the registration package, then install the Falcon package

Correct Answer: B

The correct order for manually installing a Falcon Package on a macOS system is to install the Falcon package, then register the Falcon Sensor via command line. The Falcon package contains the sensor binary and the kernel extension, while the registration package contains the customer ID and the sensor group ID. The registration package is not required for macOS systems, as the registration information can be provided via command line after installing the Falcon package1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 4

Where in the console can you find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM)?

A. Host Dashboard

B. Host Management > Filter for RFM

C. Inactive Sensor Report

D. Containment Policy

Correct Answer: B

The place in the console where you can find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM) is Host Management > Filter for RFM. The Host Management page allows you to view and manage all hosts in your environment that have Falcon sensors installed. You can use the filter bar to filter hosts by various attributes, such as status, platform, type, or group. You can also filter hosts by health events, such as RFM, which is a mode that limits the sensor\\'s functionality due to license expiration, network connectivity loss, or certificate validation failure. By filtering for RFM, you can see a list of all hosts that are in this mode1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 5

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?

A. Response Policy

B. Containment Policy

C. Maintenance Token

D. IP Allowlist Management

Correct Answer: D

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. References: 2: Cybersecurity Resources | CrowdStrike