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.passapply.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which statement is TRUE regarding disabling detections on a host?

A. Hosts with detections disabled will not alert on blocklisted hashes or machine learning detections, but will still alert on IOA-based detections. It will remain that way until detections are enabled again

B. Hosts with detections disabled will not alert on anything until detections are enabled again

C. Hosts with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

D. Hosts cannot have their detections disabled individually

Correct Answer: B

The statement that is true regarding disabling detections on a host is that hosts with detections disabled will not alert on anything until detections are enabled again. As explained in question 127, disabling detections for a host will stop the sensor from sending any detection or prevention events to the Falcon console, and remove any existing events for that host from the console. This means that the host will not alert on anything, including blocklisted hashes, machine learning detections, or indicator of attack (IOA)- based detections. The host will remain in this state until detections are enabled again1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

What can exclusions be applied to?

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

Correct Answer: B

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.

References: : [Cybersecurity Resources | CrowdStrike]

QUESTION 3

Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?

A. .*badguydomain.com.*

B. \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill

C. badguydomain\.com.*

D. Custom IOA rules cannot be created for domains

Correct Answer: A

You are usuing RegEx here and need leading ".*" to capture www and then need a ".*" at the end to identify any sites falling under badguydomain.com

QUESTION 4

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

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

Correct Answer: D

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

QUESTION 5

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