ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: CrowdStrike

Code: CCFA-200

Exam: CrowdStrike Certified Falcon Administrator

https://www.examsnest.com/exam/ccfa-200/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 5.0

Question: 1

What is the function of a single asterisk (*) in an ML exclusion pattern?

A. The single asterisk will match any number of characters, including none. It does include separator characters, such as \ or /, which separate portions of a file path
B. The single asterisk will match any number of characters, including none. It does not include separator characters, such as \ or /, which separate portions of a file path
C. The single asterisk is the insertion point for the variable list that follows the path
D. The single asterisk is only used to start an expression, and it represents the drive letter

Answer: B

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/machine-learning
The asterisk is a wildcard character that can be used in exclusion patterns to match any number of characters. However, it does not match separator characters, such as \ or /, which are used to separate portions of a file path. For example, the pattern C:\Windows**.exe will match any executable file in any subfolder of the Windows folder, but not in the Windows folder itself.
Reference: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 2

You have determined that you have numerous Machine Learning detections in your environment that are false positives. They are caused by a single binary that was custom written by a vendor for you and that binary is running on many endpoints. What is the best way to prevent these in the future?

A. Contact support and request that they modify the Machine Learning settings to no longer include this detection
B. Using IOC Management, add the hash of the binary in question and set the action to "Allow"
C. Using IOC Management, add the hash of the binary in question and set the action to "Block, hide detection"
D. Using IOC Management, add the hash of the binary in question and set the action to "No Action"

Answer: B

Explanation:

to match any number of characters including none while not matching beyond path separators (\ or /) and double asterisks are used to recursively match zero or more directories that fall under the

current directory.

Question: 3

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints
B. To define the duration of Network Containment
C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)
D. To define allowed IP addresses over which your hosts will communicate when contained

Answer: D

Explanation:

In the Containment Policy page have the title "Network traffic allowlist" and it only allows to add IPs or CIDR networks to exclude in the moment of the isolation of any host, because it is a global policy, not allowing make distinctions between machines.

Question: 4

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

A. File exclusions are not aligned to groups or hosts
B. There is a limit of three groups of hosts applied to any exclusion
C. There is no limit and exclusions can be applied to any or all groups
D. Each exclusion can be aligned to only one group of hosts

Answer: C

Explanation:

An exclusion is a rule that tells the Falcon platform to ignore certain files, folders, processes, or registry keys when performing prevention or detection actions. An administrator can create an exclusion and apply it to one or more groups of hosts, or to all hosts in the organization. For example, an administrator can create an exclusion for a legitimate application that is causing false positives and apply it to the group of hosts that are running that application.
Reference: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 5

Even though you are a Falcon Administrator, you discover you are unable to use the "Connect to Host" feature to gather additional information which is only available on the host. Which role do you need added to your user account to have this capability?

A. Real Time Responder
B. Endpoint Manager
C. Falcon Investigator

D. Remediation Manager

Answer: A

Explanation:

The Real Time Responder role allows users to use the “Connect to Host” feature to gather additional information from the host, such as running processes, registry keys, files, etc. The other roles do not have this capability. Reference: CrowdStrike Falcon User Guide, page 18.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: CrowdStrike

Code: CCFA-200

Exam: CrowdStrike Certified Falcon Administrator

https://www.examsnest.com/exam/ccfa-200/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation