CrowdStrike

CCFA-200 Exam

CrowdStrike Certified Falcon Administrator

Questions & Answers
Demo

Version: 4.0

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

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:

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: C

Explanation:

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: B

Explanation:

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: C

Thank You For Trying CCFA-200 PDF Demo

To try our CCFA-200 Premium Files visit link below:

https://examsland.com/latest-exam-questions/CCFA-200/

Start Your CCFA-200 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.