CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

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

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/machine-learning

QUESTION 2

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

A. There may be special considerations for each OS

B. To assist with testing and tracking sensor rollouts

C. The network protocols are different for each host OS

D. It is an auditing requirement

Correct Answer: D

QUESTION 3

What is the primary purpose of using glob syntax in an exclusion?

A. To specify a Domain be excluded from detections

B. To specify exclusion patterns to easily exclude files and folders and extensions from detections

C. To specify exclusion patterns to easily add files and folders and extensions to be prevented

D. To specify a network share be excluded from detections

Correct Answer: B

QUESTION 4

What are custom alerts based on?

A. Custom workflows

B. Custom event based triggers

C. Predefined alert templates

D. User defined Splunk queries

Correct Answer: B

QUESTION 5

Which of the following can a Falcon Administrator edit in an existing user\\'s profile?

A. First or Last name

B. Phone number

C. Email address

D. Working groups

Correct Answer: D