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.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

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

QUESTION 1

The Logon Activities Report includes all of the following information for a particular user EXCEPT _____.

A. the account type for the user (e.g. Domain Administrator, Local User)

B. all hosts the user logged into

C. the logon type (e.g. interactive, service)

D. the last time the user\\'s password was set

Correct Answer: B

Checked in console, it returns only the last machine where the user logged on, so it will not return all the machines that the user was logged on in the desired search

QUESTION 2

Why is it important to know your company\\'s event data retention limits in the Falcon platform?

A. This is not necessary; you simply select "All Time" in your query to search all data

B. You will not be able to search event data into the past beyond your retention period

C. Data such as process records are kept for a shorter time than event data

D. Your query will require you to specify the data pool associated with the date you wish to search

Correct Answer: B

It is important to know your company\\'s event data retention limits in the Falcon platform because you will not be able to search event data into the past beyond your retention period. The retention period is the amount of time that event data is stored in the Falcon Cloud, and it may vary depending on your subscription plan and settings. The other options are either incorrect or not related to knowing your retention limits. Reference: CrowdStrike Falcon User Guide, page 48.

QUESTION 3

What three things does a workflow condition consist of?

A. A parameter, an operator, and a value

B. A beginning, a middle, and an end

C. Triggers, actions, and alerts

D. Notifications, alerts, and API\\'s

Correct Answer: A

A workflow condition consists of a parameter, an operator, and a value. A workflow condition is a rule that defines when

a workflow should be triggered based on certain criteria or filters. A parameter is a variable or attribute that can be used to filter or match detection events, such as severity, tactic, or host group. An operator is a symbol or word that specifies how to compare or evaluate the parameter and the value, such as equals, contains, or greater than. A value is a constant or expression that provides the expected or desired result for the parameter, such as high, credential dumping, or default group1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 4

Which of the following is TRUE regarding Falcon Next-Gen AntiVirus (NGAV)?

A. Falcon NGAV relies on signature-based detections

B. Activating Falcon NGAV will also enable all detection and prevention settings in the entire policy

C. The Detection sliders cannot be set to a value less aggressive than the Prevention sliders

D. Falcon NGAV is not a replacement for Windows Defender or other antivirus programs

Correct Answer: C

The Detection sliders cannot be set to a value less aggressive than the Prevention sliders in Falcon Next-Gen AntiVirus (NGAV). This is because prevention is a subset of detection, and it would not make sense to prevent threats that are not detected. The other options are either incorrect or not true of Falcon NGAV. Reference: [CrowdStrike Falcon User Guide], page 35.

QUESTION 5

How do you find a list of inactive sensors?

A. The Falcon platform does not provide reporting for inactive sensors

B. A sensor is always considered active until removed by an Administrator

C. Run the Inactive Sensor Report in the Host setup and management option

D. Run the Sensor Aging Report within the Investigate option

Correct Answer: C

The Inactive Sensor Report in the Host setup and management option allows you to view a list of hosts that have not communicated with the Falcon platform for a specified period of time. You can filter the report by sensor version, OS, and last seen date. This report can help you identify hosts that may have connectivity issues or need sensor updates1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike