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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?

A. Sensor Report

B. Machine Learning Prevention Monitoring

C. Falcon UI Audit Trail

D. Machine Learning Debug

Correct Answer: B

The Machine Learning Prevention Monitoring report in the Prevention Policy Management option allows you to monitor the impact of machine learning (ML) prevention settings on your environment. You can view the number of ML detections and preventions by severity, policy, and host group. You can also drill down into specific events and hosts to see more details. This report can help you determine the appropriate ML levels to set in a prevention policy based on your risk tolerance and security posture1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

Where in the Falcon console can information about supported operating system versions be found?

A. Configuration module

B. Intelligence module

C. Support module

D. Discover module

Correct Answer: C

Information about supported operating system versions can be found in the Support module in the Falcon console. This module provides access to various support resources, such as documentation, downloads, FAQs, release notes and system status. One of the documents available in this module is the CrowdStrike Sensor Compatibility List, which lists the supported operating system versions for each sensor type and platform. The other options are either incorrect or not related to finding information about supported operating system versions. Reference: CrowdStrike Falcon User Guide, page 26.

QUESTION 3

Where should you look to find the history of the successes and failures for any Falcon Fusion workflows?

A. Workflow Execution log

B. Falcon Ul Audit Trail

C. Workflow Audit log

D. Custom Alert History

Correct Answer: A

The place where you can find the history of the successes and failures for any Falcon Fusion workflows is the Workflow Execution log. The Workflow Execution log in the Workflow Management option allows you to view the status and results of workflow executions triggered by detection events. You can filter the log by workflow name, status, start and end time, and detection ID. You can also view the details of each execution, including the actions performed, the output received, and any errors encountered. This log can help you troubleshoot potential failures or issues with your workflows1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 4

Which is a filter within the Host setup and management > Host management page?

A. User name

B. OU

C. BIOS Version

D. Locality

Correct Answer: B

OU (organizational unit) is a filter within the Host setup and management > Host management page. The Host management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions. You can also filter by OU, which is a logical grouping of hosts based on their Active Directory domain structure1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 5

An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?

A. The API client secret can be viewed from the Edit API client pop-up box

B. Enable the Client Secret column to reveal the API client secret

C. Re-create the API client using the exact name to see the API client secret

D. The API client secret cannot be retrieved after it has been created

Correct Answer: D

The API client secret cannot be retrieved after it has been created. The secret is only displayed once when the API client is created, and it cannot be viewed or edited later. Therefore, it is important to save the secret securely and use it along with the client ID to authenticate the API client. The other options are either incorrect or not possible. Reference: CrowdStrike Falcon User Guide, page 54.

CCFA-200 Practice Test CCFA-200 Study Guide CCFA-200 Exam Questions