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.passapply.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

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

What information does the API Audit Trail Report provide?

A. A list of analyst login activity

B. A list of specific changes to prevention policy

C. A list of actions taken via Falcon OAuth2-based APIs

D. A list of newly added hosts

Correct Answer: C

The information that the API Audit Trail Report provides is a list of actions taken via Falcon OAuth2-based APIs. The API Audit Trail Report allows you to view and audit the activity and usage of the Falcon APIs by different API clients and users in your organization. You can use this report to monitor who accessed what data, when, and how via the Falcon APIs2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 3

How do you assign a policy to a specific group of hosts?

A. Create a group containing the desired hosts using "Static Assignment." Go to the Assigned Host Groups tab of the desired policy and dick "Add groups to policy." Select the desired Group(s).

B. Assign a tag to the desired hosts in Host Management. Create a group with an assignment rule based on that tag. Go to the Assignment tab of the desired policy and click "Add Groups to Policy." Select the desired Group(s).

C. Create a group containing the desired hosts using "Dynamic Assignment." Go to the Assigned Host Groups tab of the

desired policy and select criteria such as OU, OS, Hostname pattern, etc.

D. On the Assignment tab of the desired policy, select "Static" assignment. From the next window, select the desired hosts (using fitters if needed) and click Add.

Correct Answer: A

The administrator can assign a policy to a specific group of hosts by creating a group containing the desired hosts using "Static Assignment." Then, go to the Assigned Host Groups tab of the desired policy and click "Add groups to policy." Select the desired Group(s). This will apply the policy to the selected group(s) of hosts. The other options are either incorrect or not applicable to static assignment. Reference: [CrowdStrike Falcon User Guide], page 33.

QUESTION 4

Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?

A. Next-Gen Antivirus (NGAV) protection

B. Adware and Potentially Unwanted Program detection and prevention

C. Real-time offline protection

D. Identification and analysis of unknown executables

Correct Answer: D

According to documentation (documentation/detections/technique/sensor- based-ml-cst0007): CrowdStrike sensor-based machine learning (ML) identifies and analyzes unknown executables as they run on hosts. This technique is triggered by files and file attributes associated with known malware. This is similar to the [Cloud-based ML](/support/documentation/detections/technique/cloud-based-ml) technique. Cloud-based ML is informed by global analysis of executables that classifies and identifies malware. The key difference is that it doesn\\'t run on hosts when they\\'re offline.

QUESTION 5

Which of the following controls the speed in which your sensors will receive automatic sensor updates?

A. Maintenance Tokens

B. Sensor Update Policy

C. Sensor Update Throttling

D. Channel File Update Throttling

Correct Answer: C

The option that controls the speed in which your sensors will receive automatic sensor updates is Sensor Update Throttling. Sensor Update Throttling allows you to limit the number of sensors that can download a new sensor version per hour. This way, you can avoid network congestion or bandwidth issues caused by simultaneous sensor updates. You can configure the Sensor Update Throttling setting in the Sensor Update Policy for each platform1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Latest CCFA-200 Dumps CCFA-200 Practice Test CCFA-200 Exam Questions