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.leads4pass.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

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: C

QUESTION 2

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell

C. Yara

D. Regex

Correct Answer: B

QUESTION 3

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions

during the testing phase.

What settings do you choose?

A. Detection slider: Extra Aggressive Prevention slider: Cautious

B. Detection slider: Moderate Prevention slider: Disabled

C. Detection slider: Cautious Prevention slider: Cautious

D. Detection slider: Disabled Prevention slider: Disabled

Correct Answer: C

QUESTION 4

What model is used to create workflows that would allow you to create custom notifications based on particular events which occur in the Falcon platform?

A. For - While statement(s)

B. Trigger, condition(s) and action(s)

C. Event trigger(s)

D. Predefined workflow template(s)

Correct Answer: B

QUESTION 5

Which role allows a user to connect to hosts using Real-Time Response?

A. Endpoint Manager

B. Falcon Administrator

C. Real Time Responder ?Active Responder

D. Prevention Hashes Manager

Correct Answer: C