VCE & PDF
Pass4itSure.com

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 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

QUESTION 2

What impact does disabling detections on a host have on an API?

A. Endpoints with detections disabled will not alert on anything until detections are enabled again

B. Endpoints cannot have their detections disabled individually

C. DetectionSummaryEvent stops sending to the Streaming API for that host

D. Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

Correct Answer: D

QUESTION 3

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints

B. To define the duration of Network Containment

C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)

D. To define allowed IP addresses over which your hosts will communicate when contained

Correct Answer: C

QUESTION 4

Which role is required to manage groups and policies in Falcon?

A. Falcon Host Analyst

B. Falcon Host Administrator

C. Prevention Hashes Manager

D. Falcon Host Security Lead

Correct Answer: B

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: D

Latest CCFA-200 Dumps   CCFA-200 PDF Dumps   CCFA-200 VCE Dumps