CCFA-200$^{\text{Q\&As}}$

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

How does the Unique Hosts Connecting to Countries Map help an administrator?

A. It highlights countries with known malware

B. It helps visualize global network communication

C. It identifies connections containing threats

D. It displays intrusions from foreign countries

Correct Answer: B

QUESTION 2

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 3

Your CISO has decided all Falcon Analysts should also have the ability to view files and file contents locally on compromised hosts, but without the ability to take them off the host. What is the most appropriate role that can be added to fullfil this requirement?

A. Remediation Manager

B. Real Time Responder ?Read Only Analyst

C. Falcon Analyst ?Read Only

D. Real Time Responder ?Active Responder

Correct Answer: C

QUESTION 4

You are evaluating the most appropriate Prevention Policy Machine Learning slider settings for your environment. In your testing phase, you configure the Detection slider as Aggressive. After running the sensor with this configuration for

1 week of testing, which Audit report should you review to determine the best Machine Learning slider settings for your organization?

A. Prevention Policy Audit Trail

B. Prevention Policy Debug

C. Prevention Hashes Ignored

D. Machine-Learning Prevention Monitoring

Correct Answer: A

QUESTION 5

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?

A. Falcon console updates are pending

B. Falcon sensors installing an update

C. Notifications have been disabled on that host sensor

D. Microsoft updates

Correct Answer: C