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

QUESTION 1

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?

A. SSL inspection should be configured to occur on all Falcon traffic

B. Some network configurations, such as deep packet inspection, interfere with certificate validation

C. HTTPS interception should be enabled to proceed with certificate validation

D. Common sources of interference with certificate pinning include protocol race conditions and resource contention

Correct Answer: B

The statement that some network configurations, such as deep packet inspection, interfere with certificate validation is true concerning Falcon sensor certificate validation. The Falcon sensor uses certificate pinning to defend against man-inthe-middle attacks, which means that it verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. Some network configurations, such as deep packet inspection, SSL inspection, or HTTPS interception, may attempt to modify or replace the server certificate, which will cause the sensor to reject the connection and generate an error3. References: 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 2

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

The Unique Hosts Connecting to Countries Map helps an administrator to visualize global network communication. The map shows the number of unique hosts in your environment that have established network connections to different countries in the past 24 hours. You can use this map to identify unusual or suspicious network activity, such as connections to high-risk countries or regions, or connections from hosts that are not expected to communicate with external entities2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 3

How do you disable all detections for a host?

A. Create an exclusion rule and apply it to the machine or group of machines

B. Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)

C. You cannot disable all detections on individual hosts as it would put them at risk

D. In Host Management, select the host and then choose the option to Disable Detections

Correct Answer: D

The administrator can disable all detections for a host by selecting the host and then choosing the option to Disable Detections in the Host Management page. This will prevent the host from sending any detection events to the Falcon Cloud. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 32.

QUESTION 4

A sensor that has not contacted the Falcon cloud will be automatically deleted from the hosts list after how many days?

A. 45 Days

B. 60 Days

C. 30 Days

D. 90 Days

Correct Answer: D

A sensor that has not contacted the Falcon cloud will be automatically deleted from the hosts list after 90 days. A sensor that has not contacted the Falcon cloud for more than seven days is considered inactive and will be moved from the Host Management page to the Trash page. An inactive sensor will remain in the Trash page for 90 days before being permanently deleted from the Falcon platform. You can restore an inactive sensor from the Trash page if it contacts the Falcon cloud again within 90 days. References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

QUESTION 5

You have an existing workflow that is triggered on a critical detection that sends an email to the escalation team. Your CISO has asked to also be notified via email with a customized message. What is the best way to update the workflow?

A. Clone the workflow and replace the existing email with your CISO\\'s email

B. Add a sequential action to send a custom email to your CISO

C. Add a parallel action to send a custom email to your CISO

D. Add the CISO\\'s email to the existing action

Correct Answer: C

The best way to update the workflow is to add a parallel action to send a custom email to your CISO. A parallel action allows you to perform multiple actions simultaneously when a workflow is triggered, without affecting the order or outcome of other actions. A sequential action, on the other hand, requires one action to complete before another action can start. By adding a parallel action, you can ensure that both the escalation team and your CISO receive an email notification as soon as possible1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

CCFA-200 PDF Dumps CCFA-200 Study Guide CCFA-200 Braindumps