DUMPSARENA

CrowdStrike Certified Falcon Administrator

CrowdStrike CCFA-200

Version Demo

Total Demo Questions: 10

Total Premium Questions: 96

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Your organization has a set of servers that are not allowed to be accessed remotely, including via Real Time Response (RTR). You already have these servers in their own Falcon host group. What is the next step to disable RTR only on these hosts?

A. Edit the Default Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

B. Edit the Default Response Policy and add the host group to the exceptions list under "Real Time Functionality"

C. Create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

D. Create a new Response Policy and add the host name to the exceptions list under "Real Time Functionality"

ANSWER: C

QUESTION NO: 2

How long are detection events kept in Falcon?

A. Detection events are kept for 90 days

B. Detections events are kept for your subscribed data retention period

C. Detection events are kept for 7 days

D. Detection events are kept for 30 days

ANSWER: B

QUESTION NO: 3

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

A. Older versions of the sensor are not available for download

B. By emailing CrowdStrike support at support@crowdstrike.com

C. By installing the current sensor and clicking the "downgrade" button during the install

D. By clicking on "Older versions" links under the Host setup and management > Deploy > Sensor downloads

ANSWER: D

QUESTION NO: 4

An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?

A. The API client secret can be viewed from the Edit API client pop-up box

B. Enable the Client Secret column to reveal the API client secret

C. Re-create the API client using the exact name to see the API client secret

D. The API client secret cannot be retrieved after it has been created

ANSWER: B

QUESTION NO: 5

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?

A. TCP port 22 (SSH)

B. TCP port 443 (HTTPS)

C. TCP port 80 (HTTP)

D. TCP UDP port 53 (DNS)

ANSWER: B

QUESTION NO: 6

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

ANSWER: B

QUESTION NO: 7

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

ANSWER: B

QUESTION NO: 8

Once an exclusion is saved, what can be edited in the future?

A. All parts of the exclusion can be changed

B. Only the selected groups and hosts to which the exclusion is applied can be changed

C. Only the options to "Detect/Block" and/or "File Extraction" can be changed

D. The exclusion pattern cannot be changed

ANSWER: B

QUESTION NO: 9

In order to quarantine files on the host, what prevention policy settings must be enabled?

A. Malware Protection and Custom Execution Blocking must be enabled

B. Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration" must be enabled

C. Malware Protection and Windows Anti-Malware Execution Blocking must be enabled

D. Behavior-Based Threat Prevention sliders and Advanced Remediation Actions must be enabled

ANSWER: C

QUESTION NO: 10

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

ANSWER: D