CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?

A. Sensor Report

B. Machine Learning Prevention Monitoring

C. Falcon UI Audit Trail

D. Machine Learning Debug

Correct Answer: B

QUESTION 2

What is the primary purpose of using glob syntax in an exclusion?

A. To specify a Domain be excluded from detections

B. To specify exclusion patterns to easily exclude files and folders and extensions from detections

C. To specify exclusion patterns to easily add files and folders and extensions to be prevented

D. To specify a network share be excluded from detections

Correct Answer: B

QUESTION 3

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

QUESTION 4

Which of the following is a valid step when troubleshooting sensor installation failure?

A. Confirm all required services are running on the system

B. Enable the Windows firewall

C. Disable SSL and TLS on the host

D. Delete any available application crash log files

Correct Answer: A

QUESTION 5

The alignment of a particular prevention policy to one or more host groups can be completed in which of the following locations within Falcon?

A. Policy alignment is configured in the "Host Management" section in the Hosts application

B. Policy alignment is configured only once during the initial creation of the policy in the "Create New Policy" pop-up window

C. Policy alignment is configured in the General Settings section under the Configuration menu

D. Policy alignment is configured in each policy in the "Assigned Host Groups" tab

Correct Answer: D

QUESTION 6

The Logon Activities Report includes all of the following information for a particular user EXCEPT __________.

A. the account type for the user (e.g. Domain Administrator, Local User)

B. all hosts the user logged into

C. the logon type (e.g. interactive, service)

D. the last time the user\\'s password was set

Correct Answer: D

QUESTION 7

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 8

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

Correct Answer: B

QUESTION 9

On which page of the Falcon console would you create sensor groups?

A. User management

B. Sensor update policies

C. Host management

D. Host groups

Correct Answer: D

QUESTION 10

What information is provided in Logan Activities under Visibility Reports?

A. A list of all logons for all users

B. A list of last endpoints that a user logged in to

C. A list of users who are remotely logged on to devices based on local IP and local port

D. A list of unique users who are remotely logged on to devices based on the country

Correct Answer: B

QUESTION 11

Which of the following is NOT an available filter on the Hosts Management page?

A. Hostname

B. Username

C. Group

D. OS Version

Correct Answer: D

QUESTION 12

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: B

QUESTION 13

Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?

A. .*badguydomain.com.*

B. \Device\HarddiskVolume2\*.exe -SingleArgument www.badguydomain.com /kill

C. badguydomain\.com.*

D. Custom IOA rules cannot be created for domains

Correct Answer: B

QUESTION 14

Where do you obtain the Windows sensor installer for CrowdStrike Falcon?

A. Sensors are downloaded from the Hosts > Sensor Downloads

B. Sensor installers are unique to each customer and must be obtained from support

C. Sensor installers are downloaded from the Support section of the CrowdStrike website

D. Sensor installers are not used because sensors are deployed from within Falcon

Correct Answer: B

QUESTION 15

Which exclusion pattern will prevent detections on a file at C:\Program Files\My Program\My Files\program.exe?

A. \Program Files\My Program\My Files*

B. \Program Files\My Program*

C. **

D. *\Program Files\My Program*\

Correct Answer: A

[Latest CCFA-200 Dumps](https://www.leads4pass.com/ccfa-200.html) [CCFA-200 PDF Dumps](https://www.leads4pass.com/ccfa-200.html) [CCFA-200 Exam Questions](https://www.leads4pass.com/ccfa-200.html)