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

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

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

Correct Answer: B

QUESTION 2

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"

Correct Answer: C

QUESTION 3

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell

C. Yara

D. Regex

Correct Answer: B

QUESTION 4

When creating new IOCs in IOC management, which of the following fields must be configured?

A. Hash, Description, Filename

B. Hash, Action and Expiry Date

C. Filename, Severity and Expiry Date

D. Hash, Platform and Action

Correct Answer: D

QUESTION 5

How do you assign a policy to a specific group of hosts?

A. Create a group containing the desired hosts using "Static Assignment." Go to the Assigned Host Groups tab of the desired policy and dick "Add groups to policy." Select the desired Group(s).

B. Assign a tag to the desired hosts in Host Management. Create a group with an assignment rule based on that tag. Go to the Assignment tab of the desired policy and click "Add Groups to Policy." Select the desired Group(s).

C. Create a group containing the desired hosts using "Dynamic Assignment." Go to the Assigned Host Groups tab of the desired policy and select criteria such as OU, OS, Hostname pattern, etc.

D. On the Assignment tab of the desired policy, select "Static" assignment. From the next window, select the desired hosts (using fitters if needed) and click Add.

Correct Answer: C

QUESTION 6

You are attempting to install the Falcon sensor on a host with a slow Internet connection and the installation fails after 20 minutes. Which of the following parameters can be used to override the 20 minute default provisioning window?

A. ExtendedWindow=1

B. Timeout=0

C. ProvNoWait=1

D. Timeout=30

Correct Answer: D

QUESTION 7

Which of the following is TRUE of the Logon Activities Report?

A. Shows a graphical view of user logon activity and the hosts the user connected to

B. The report can be filtered by computer name

C. It gives a detailed list of all logon activity for users

D. It only gives a summary of the last logon activity for users

Correct Answer: C

QUESTION 8

Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?

A. Next-Gen Antivirus (NGAV) protection

B. Adware and Potentially Unwanted Program detection and prevention

C. Real-time offline protection

D. Identification and analysis of unknown executables

Correct Answer: D

QUESTION 9

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

QUESTION 10

While a host is Network contained, you need to allow the host to access internal network resources on specific IP addresses to perform patching and remediation. Which configuration would you choose?

A. Configure a Real Time Response policy allowlist with the specific IP addresses

B. Configure a Containment Policy with the specific IP addresses

C. Configure a Containment Policy with the entire internal IP CIDR block D. Configure the Host firewall to allowlist the specific IP addresses

Correct Answer: D

QUESTION 11

Where can you modify settings to permit certain traffic during a containment period?

A. Prevention Policy

B. Host Settings

C. Containment Policy

D. Firewall Settings

Correct Answer: C

QUESTION 12

What command should be run to verify if a Windows sensor is running?

A. regedit myfile.reg

B. sc query csagent

C. netstat -f

D. ps -ef | grep falcon

Correct Answer: B

QUESTION 13

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

Correct Answer: B

QUESTION 14

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 15

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions

during the testing phase.

What settings do you choose?

A. Detection slider: Extra Aggressive Prevention slider: Cautious

B. Detection slider: Moderate Prevention slider: Disabled

C. Detection slider: Cautious Prevention slider: Cautious

D. Detection slider: Disabled Prevention slider: Disabled

Correct Answer: C

Latest CCFA-200 Dumps CCFA-200 Practice Test CCFA-200 Study Guide