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

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

QUESTION 1

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 2

When a host is placed in Network Containment, which of the following is TRUE?

A. The host machine is unable to send or receive network traffic outside of the local network

B. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and traffic allowed in the Firewall Policy

C. The host machine is unable to send or receive any network traffic

D. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and any resources allowlisted in the Containment Policy

Correct Answer: D

QUESTION 3

What can the Quarantine Manager role do?

A. Manage and change prevention settings

B. Manage quarantined files to release and download

C. Manage detection settings

D. Manage roles and users

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

What type of information is found in the Linux Sensors Dashboard?

A. Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage

B. Hidden File execution, Execution of file from the trash, Versions Running with Computer Names

C. Versions running, Directory Made Invisible to Spotlight, Logging/Auditing Referenced, Viewed, or Modified

D. Private Information Accessed, Archiving Tools ?Exfil, Files Made Executable

Correct Answer: C

QUESTION 6

Which of the following best describes the Default Sensor Update policy?

A. The Default Sensor Update policy does not have the "Uninstall and maintenance protection" feature

B. The Default Sensor Update policy is only used for testing sensor updates

C. The Default Sensor Update policy is a "catch-all" policy

D. The Default Sensor Update policy is disabled by default

Correct Answer: C

QUESTION 7

Under the "Next-Gen Antivirus: Cloud Machine Learning" setting there are two categories, one of them is "Cloud Anti-Malware" and the other is:

A. Adware and PUP

B. Advanced Machine Learning

C. Sensor Anti-Malware

D. Execution Blocking

Correct Answer: B

QUESTION 8

When creating an API client, which of the following must be saved immediately since it cannot be viewed again after the client is created?

A. Base URL

B. Secret

C. Client ID

D. Client name

Correct Answer: B

QUESTION 9

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints

B. To define the duration of Network Containment

C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)

D. To define allowed IP addresses over which your hosts will communicate when contained

Correct Answer: C

QUESTION 10

What is the purpose of precedence with respect to the Sensor Update policy?

A. Precedence applies to the Prevention policy and not to the Sensor Update policy

B. Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)

C. Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)

D. Precedence ensures that conflicting policy settings are not set in the same policy

Correct Answer: B

QUESTION 11

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from uninstalling or upgrading the sensor, which settings in the Sensor Update Policy would meet this criteria?

A. Sensor version set to N-1 and Bulk maintenance mode is turned on

B. Sensor version fixed and Uninstall and maintenance protection turned on

C. Sensor version updates off and Uninstall and maintenance protection turned off

D. Sensor version set to N-2 and Bulk maintenance mode is turned on

Correct Answer: B

QUESTION 12

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 13

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 14

What is the name for the unique host identifier in Falcon assigned to each sensor during sensor installation?

A. Endpoint ID (EID)

B. Agent ID (AID)

C. Security ID (SID)

D. Computer ID (CID)

Correct Answer: B

QUESTION 15

What are custom alerts based on?

A. Custom workflows

B. Custom event based triggers

C. Predefined alert templates

D. User defined Splunk queries

Correct Answer: B