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

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

The command that should be run to verify if a Windows sensor is running is sc query csagent. This command will display the status and information of the csagent service, which is the Falcon sensor service. The other commands are either incorrect or not applicable to Windows sensors. Reference: [CrowdStrike Falcon User Guide], page 29.

QUESTION 2

To enhance your security, you want to detect and block based on a list of domains and IP addresses. How can you use IOC management to help this objective?

A. Blocking of Domains and IP addresses is not a function of IOC management. A Custom IOA Rule should be used instead

B. Using IOC management, import the list of hashes and IP addresses and set the action to Detect Only

C. Using IOC management, import the list of hashes and IP addresses and set the action to Prevent/Block

D. Using IOC management, import the list of hashes and IP addresses and set the action to No Action

Correct Answer: A

IOC management only allows "Detect only" and "No Action" among the possible actions. Therefore, it cannot be used to block based on IPs or domains. Custom IOA Rule groups allow to create rule types based on Network Connection (configuring a remote IP address) and domains, and gives the options to "Monitor", "Detect" and "Kill Process", being the late one the closest to "block".

QUESTION 3

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

A valid step when troubleshooting sensor installation failure is to confirm all required services are running on the system. This can help identify if there are any issues with the sensor service, the Windows Management Instrumentation service, or the Windows Remote Management service, which are required for the sensor to function properly. The other options are either incorrect or not helpful for troubleshooting sensor installation failure. Reference: CrowdStrike Falcon User Guide, page 29.

QUESTION 4

An inactive host that does not contact the Falcon cloud will be automatically removed from the Host Management and Trash pages after how many days?

A. 45 Days

B. 60 Days

C. 75 Days

D. 90 Days

Correct Answer: D

An inactive host that does not contact the Falcon cloud will be automatically removed from the Host Management and Trash pages after 90 days. An inactive host is a host that has not communicated with the Falcon platform for more than seven days. An inactive host will be moved from the Host Management page to the Trash page after seven days of inactivity. An inactive host will remain in the Trash page for 90 days before being permanently deleted from the Falcon platform. You can restore an inactive host from the Trash page if it becomes active again within 90 days1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 5

What best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page?

A. The detections for the host are removed from the console immediately and no new detections will display in the console going forward

B. You cannot disable detections for a host

C. Existing detections for the host remain, but no new detections will display in the console going forward

D. Preventions will be disabled for the host

Correct Answer: A

The option that best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page is that the detections for the host are removed from the console immediately and no new detections will display in the console going forward. The "Disable Detections" feature allows you to enable or disable the detection and prevention capabilities of the Falcon sensor on a specific host. When you disable detections for a host, the sensor will stop sending any detection or prevention events to the Falcon console, and any existing events for that host will be removed from the console. When you enable detections for a host, the sensor will resume sending any new detection or prevention events to the Falcon console, but any previous events for that host will not be

restored to the console1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 6

With Custom Alerts, it is possible to _____.

A. schedule the alert to run at any interval

B. receive an alert in an email

C. configure prevention actions for alerting

D. be alerted to activity in real-time

Correct Answer: B

The reporting interval is predefined and cannot be changed. You can only enable/disable the custom alert feature and add/remove recipient email client for the alert/detection.

QUESTION 7

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 8

When a host belongs to more than one host group, how is sensor update precedence determined?

A. Groups have no impact on sensor update policies

B. Sensors of hosts that belong to more than one group must be manually updated

C. The highest precedence policy from the most important group is applied to the host

D. All of the host\\'s groups are examined in aggregate and the policy with highest precedence is applied to the host

Correct Answer: D

The option that describes how sensor update precedence is determined when a host belongs to more than one host group is that all of the host\\'s groups are examined in aggregate and the policy with highest precedence is applied to the host. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. You can create and assign custom Sensor Update policies to different hosts or groups in your environment. Each Sensor Update policy has a precedence value, which determines its priority over other policies. The higher the precedence value, the higher the priority. If a host belongs to more than one host group, each with a different Sensor Update policy assigned, then all of the host\\'s groups are examined in aggregate and the policy with highest precedence among them is applied to the host. References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

QUESTION 9

The Customer ID (CID) is important in which of the following scenarios?

A. When adding a user to the Falcon console under the Users application

B. When performing the sensor installation process

C. When setting up API keys

D. When performing a Host Search

Correct Answer: B

The Customer ID (CID) is important in which of the following scenarios: when performing the sensor installation process and when setting up API keys. The CID is a unique identifier for your organization that is required for authenticating your sensor installation and communication with the Falcon cloud. You need to provide your CID when installing the Falcon sensor on a host, either by using a command-line parameter or by using the falconctl tool. The CID is also required for setting up API keys, which are used for accessing the Falcon platform programmatically via the Falcon APIs. You need to provide your CID when creating an API client and key in the API Clients and Keys page in the Falcon console. References: : [Cybersecurity Resources | CrowdStrike]

QUESTION 10

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

A. There may be special considerations for each OS

B. To assist with testing and tracking sensor rollouts

C. The network protocols are different for each host OS

D. It is an auditing requirement

Correct Answer: A

https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in- falcon/

QUESTION 11

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: A

The type of information that is found in the Linux Sensors Dashboard is Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage. The Linux Sensors Dashboard is a dashboard that provides an overview of the Linux hosts in your environment that have Falcon sensors installed. You can use this dashboard to monitor the health and activity of your Linux hosts, such as their kernel versions, root shell usage, network communication, detections, and preventions. References: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 12

Which of the following is NOT an available action for an API Client?

A. Edit an API Client

B. Reset an API Client Secret

C. Retrieve an API Client Secret

D. Delete an API Client

Correct Answer: C

The option that is not an available action for an API Client is Retrieve an API Client Secret. An API Client is an entity that represents a user or application that can access the Falcon platform programmatically via the Falcon APIs. An API Client has an API Client ID and an API Client Secret, which are used for authenticating and authorizing API requests. You can create and manage API Clients in the API Clients and Keys page in the Falcon console. The available actions for an API Client are Edit an API Client, Reset an API Client Secret, and Delete an API Client. You cannot retrieve an API Client Secret after it has been created, as it is only displayed once during creation for security reasons2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 13

Which of the following controls the speed in which your sensors will receive automatic sensor updates?

A. Maintenance Tokens

B. Sensor Update Policy

C. Sensor Update Throttling

D. Channel File Update Throttling

Correct Answer: C

The option that controls the speed in which your sensors will receive automatic sensor updates is Sensor Update Throttling. Sensor Update Throttling allows you to limit the number of sensors that can download a new sensor version per hour. This way, you can avoid network congestion or bandwidth issues caused by simultaneous sensor updates. You can configure the Sensor Update Throttling setting in the Sensor Update Policy for each platform1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 14

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 15

What is the maximum number of patterns that can be added when creating a new exclusion?

A. 10

B. 0

C. 1

D. 5

Correct Answer: C

The maximum number of patterns that can be added when creating a new exclusion is one. Each exclusion can only have one pattern, which can be a file path, a hash, a command line or a user name. The other options are either incorrect or not related to creating exclusions. Reference: CrowdStrike Falcon User Guide, page 37.

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