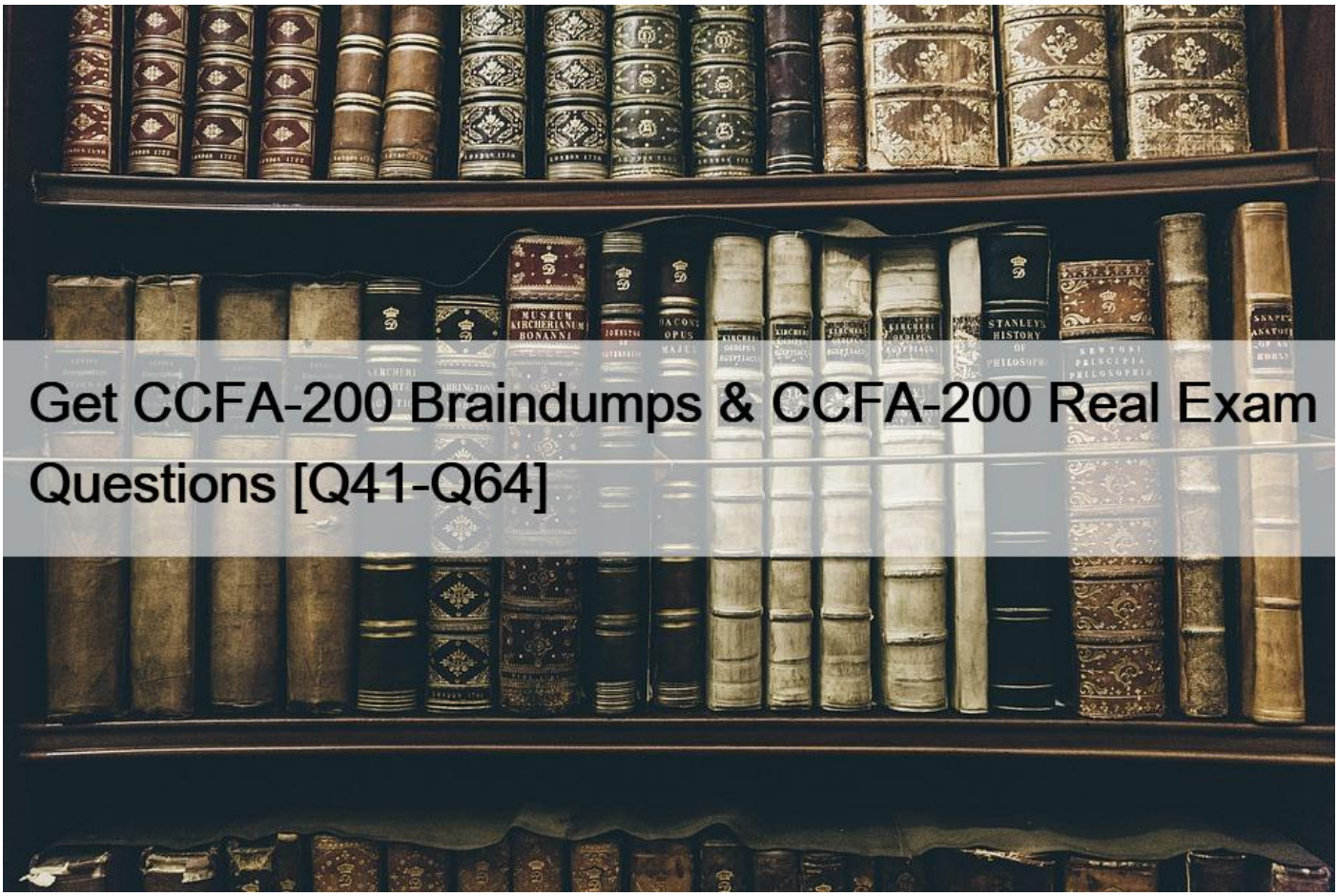
Get CCFA-200 Braindumps & CCFA-200 Real Exam Questions [Q41-Q64



Get CCFA-200 Braindumps & CCFA-200 Real Exam Questions
CrowdStrike CCFA-200 Actual Questions and Braindumps

CrowdStrike CCFA-200 exam is a comprehensive assessment of an individual's knowledge of the CrowdStrike Falcon platform. CCFA-200 exam covers a wide range of topics, including the basics of endpoint protection, malware analysis, threat intelligence, and incident response. CCFA-200 exam also tests the individual's ability to configure, operate, and troubleshoot the CrowdStrike Falcon platform. CCFA-200 exam consists of 60 multiple-choice questions and is timed at 90 minutes. Passing the exam requires a score of 70% or higher.

QUESTION 41

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?
* Blocking of Domains and IP addresses is not a function of IOC management. A Custom IOA Rule should be used instead
* Using IOC management, import the list of hashes and IP addresses and set the action to Detect Only
* Using IOC management, import the list of hashes and IP addresses and set the action to Prevent/Block

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

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 42

Which of the following pages provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System?
* Support and resources
* Activity Overview
* Hosts Overview
* Sensor Health
Explanation

The page that provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System is Sensor Health. The Sensor Health page allows you to view and monitor the health and status of all sensors in your environment. You can use this page to identify any sensors that have issues or errors, such as RFM, which is a mode that limits the sensor’s functionality due to license expiration, network connectivity loss, or certificate validation failure. You can filter the sensors by operating system, sensor version, last seen date, health events, detections, and preventions3.

References: 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 43

What best describes what happens to detections in the console after clicking “Disable Detections” for a host from within the Host Management page?
* The detections for the host are removed from the console immediately and no new detections will display in the console going forward
* You cannot disable detections for a host
* Existing detections for the host remain, but no new detections will display in the console going forward
* Preventions will be disabled for the host
Explanation

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 44

What can exclusions be applied to?

* Individual hosts selected by the administrator
* Either all hosts or specified groups
* Only the default host group
* Only the groups selected by the administrator

Explanation

The option that describes what exclusions can be applied to is that exclusions can be applied to either all hosts or specified groups. An exclusion is a rule that defines what files, folders, processes, IP addresses, or domains should be excluded from detection or prevention by the Falcon sensor. You can create and manage exclusions in the Exclusions page in the Falcon console. You can apply exclusions to either all hosts in your environment or to specific host groups that you select. You cannot apply exclusions to individual hosts selected by the administrator.

References: : [Cybersecurity Resources | CrowdStrike]

QUESTION 45

Custom IOA rules are defined using which syntax?

* Glob
* PowerShell
* Yara
* Regex

QUESTION 46

Where can you find your company’s Customer ID (CID)?

* The CID is a secret key used for Falcon communication and is never shared with the customer
* The CID is only available by calling support
* The CID is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the checksum
* The CID is located at Hosts > Host Management

Explanation

The CID (Customer ID) is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the checksum. The CID is a unique identifier for your organization that is required for authenticating your sensor installation and communication with the Falcon cloud. The checksum is a value that verifies the integrity of the sensor download file. You can find your CID and checksum at the top of the Sensor Downloads page1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 47

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

* Confirm all required services are running on the system
* Enable the Windows firewall
* Disable SSL and TLS on the host
* Delete any available application crash log files

Explanation

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 48

Which of the following best describes the Default Sensor Update policy?
* The Default Sensor Update policy does not have the “Uninstall and maintenance protection” feature
* The Default Sensor Update policy is only used for testing sensor updates
* The Default Sensor Update policy is a “catch-all” policy
* The Default Sensor Update policy is disabled by default
Explanation

The Default Sensor Update policy is a “catch-all” policy. This means that any host that is not assigned to a specific sensor update policy will inherit the settings from the Default Sensor Update policy. The Default Sensor Update policy is enabled by default and has the “Uninstall and maintenance protection” feature turned on. You can modify the settings of the Default Sensor Update policy, but you cannot delete or disable it2.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 49

Which statement is TRUE regarding disabling detections on a host?
* Hosts with detections disabled will not alert on blocklisted hashes or machine learning detections, but will still alert on lOA-based detections. It will remain that way until detections are enabled again
* Hosts with detections disabled will not alert on anything until detections are enabled again
* Hosts with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed
* Hosts cannot have their detections disabled individually
Explanation

The statement that is true regarding disabling detections on a host is that hosts with detections disabled will not alert on anything until detections are enabled again. As explained in question 127, disabling detections for a host will stop the sensor from sending any detection or prevention events to the Falcon console, and remove any existing events for that host from the console. This means that the host will not alert on anything, including blocklisted hashes, machine learning detections, or indicator of attack (IOA)-based detections. The host will remain in this state until detections are enabled again1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 50

Which role will allow someone to manage quarantine files?
* Falcon Security Lead
* Detections Exceptions Manager
* Falcon Analyst – Read Only
* Endpoint Manager
Explanation

The role that will allow someone to manage quarantine files is Falcon Security Lead. This role allows users to view and manage quarantined files, as well as release them from quarantine or download them for further analysis. The other roles do not have this capability. Reference: CrowdStrike Falcon User Guide, page 19.

QUESTION 51

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?
* TCP port 22 (SSH)
* TCP port 443 (HTTPS)
* TCP port 80 (HTTP)
* TCP UDP port 53 (DNS)

Explanation

The sensor uses TCP port 443 (HTTPS) to communicate with the CrowdStrike Cloud. This port and protocol are used to securely send and receive data between the sensor and the cloud, such as detections, policies, updates, commands, etc. The other options are either incorrect or not used by the sensor.

Reference: CrowdStrike Falcon User Guide, page 28.

QUESTION 52

Where can you modify settings to permit certain traffic during a containment period?
* Prevention Policy
* Host Settings
* Containment Policy
* Firewall Settings

QUESTION 53

What command should be run to verify if a Windows sensor is running?
* regedit myfile.reg
* sc query csagent
* netstat -f
* ps -ef | grep falcon

Explanation

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 54

What three things does a workflow condition consist of?
* A parameter, an operator, and a value
* A beginning, a middle, and an end
* Triggers, actions, and alerts
* Notifications, alerts, and API’s

Explanation

A workflow condition consists of a parameter, an operator, and a value. A workflow condition is a rule that defines when a workflow should be triggered based on certain criteria or filters. A parameter is a variable or attribute that can be used to filter or match detection events, such as severity, tactic, or host group. An operator is a symbol or word that specifies how to compare or evaluate the parameter and the value, such as equals, contains, or greater than. A value is a constant or expression that provides the expected or desired result for the parameter, such as high, credential dumping, or default group1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 55

Which of the following is NOT an available filter on the Hosts Management page?
* Hostname
* Username
* Group
* OS Version
Explanation

Username is not an available filter on the Hosts Management page. The Hosts Management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions. You can also perform actions such as assigning hosts to groups, updating sensor policies, uninstalling sensors, or isolating hosts1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 56

How do you find a list of inactive sensors?
* The Falcon platform does not provide reporting for inactive sensors
* A sensor is always considered active until removed by an Administrator
* Run the Inactive Sensor Report in the Host setup and management option
* Run the Sensor Aging Report within the Investigate option
Explanation

The Inactive Sensor Report in the Host setup and management option allows you to view a list of hosts that have not communicated with the Falcon platform for a specified period of time. You can filter the report by sensor version, OS, and last seen date. This report can help you identify hosts that may have connectivity issues or need sensor updates1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 57

What is likely the reason your Windows host would be in Reduced Functionality Mode (RFM)?
* Microsoft updates altering the kernel
* The host lost internet connectivity
* A misconfiguration in your prevention policy for the host
* A Sensor Update Policy was misconfigured
Explanation

The likely reason your Windows host would be in Reduced Functionality Mode (RFM) is that the host lost internet connectivity. RFM is a mode that limits the sensor’s functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud1. Losing internet connectivity is a common cause of RFM, as it prevents the sensor from communicating with the Falcon cloud. A misconfiguration in your prevention policy or sensor update policy will not cause RFM, as these policies are applied by the Falcon cloud and do not affect the sensor’s license, network, or certificate status. Microsoft updates altering the kernel may cause compatibility

issues with the sensor, but not RFM3.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 58

How can a Falcon Administrator configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity?
* By ensuring each user has set the “pop-ups allowed” in their User Profile configuration page
* By enabling “Upload quarantined files” in the General Settings configuration page
* By turning on the “Notify End Users” setting at the top of the Prevention policy details configuration page
* By selecting “Enable pop-up messages” from the User configuration page
Explanation

A Falcon Administrator can configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity by turning on the “Notify End Users” setting at the top of the Prevention policy details configuration page. This setting allows users to enable or disable end user notifications for prevention actions taken by Falcon on Windows hosts. The other options are either incorrect or not related to configuring pop-up messages. Reference: CrowdStrike Falcon User Guide, page 36.

QUESTION 59

How do you assign a Prevention policy to one or more hosts?
* Create a new policy and assign it directly to those hosts on the Host Management page
* Modify the users roles on the User Management page
* Ensure the hosts are in a group and assign that group to a custom Prevention policy
* Create a new policy and assign it directly to those hosts on the Prevention policy page
Explanation

The administrator can assign a Prevention policy to one or more hosts by ensuring the hosts are in a group and assigning that group to a custom Prevention policy. This allows users to apply different prevention settings and options to different groups of hosts based on their needs and preferences. The other options are either incorrect or not applicable to assigning a Prevention policy. Reference: [CrowdStrike Falcon User Guide], page 34.

QUESTION 60

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?
* TCP port 22 (SSH)
* TCP port 443 (HTTPS)
* TCP port 80 (HTTP)
* TCP UDP port 53 (DNS)

QUESTION 61

What should be disabled on firewalls so that the sensor’s man-in-the-middle attack protection works properly?
* Deep packet inspection
* Linux Sub-System
* PowerShell
* Windows Proxy

Explanation

The option that should be disabled on firewalls so that the sensor’s man-in-the-middle attack protection works properly is deep packet inspection. Deep packet inspection is a network configuration that inspects and modifies the data packets that pass through a firewall. Deep packet inspection may interfere with the sensor’s certificate validation, which is a feature that verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. If the certificate validation fails, the sensor will reject the connection and generate an error3.

References: 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 62

What impact does disabling detections on a host have on an API?
* Endpoints with detections disabled will not alert on anything until detections are enabled again
* Endpoints cannot have their detections disabled individually
* DetectionSummaryEvent stops sending to the Streaming API for that host
* Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

QUESTION 63

What best describes what happens to detections in the console after clicking “Enable Detections” for a host which previously had its detections disabled?
* Enables custom detections for the host
* New detections will start appearing in the console, and all retroactive stored detections will be restored to the console for that host
* New detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host
* Preventions will be enabled for the host

Explanation

The option that best describes what happens to detections in the console after clicking “Enable Detections” for a host which previously had its detections disabled is that new detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host. The “Enable 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 64

Why would you assign hosts to a static group instead of a dynamic group?
* You do not want the group membership to change automatically
* You are managing more than 1000 hosts
* You need hosts to be automatically assigned to a group
* You want the group to contain hosts from multiple operating systems

CCFA-200 Dumps To Pass CrowdStrike Exam in 24 Hours - Test4Engine:
https://www.test4engine.com/CCFA-200_exam-latest-braindumps.html]