[Mar-2025 CCFA-200 Exam Dumps - Free Demo & 365 Day Updates [Q56-Q74

[Mar-2025] CCFA-200 Exam Dumps - Free Demo & 365 Day Updates
Free Sales Ending Soon - Use Real CCFA-200 PDF Questions

CrowdStrike CCFA-200 Exam is a vendor-neutral certification, meaning that it is not tied to a specific technology or product. This makes it a valuable credential for IT professionals who are looking to expand their knowledge and skills in endpoint security. CCFA-200 exam is also recognized by other industry certifications, such as CompTIA, and can be used to fulfill continuing education requirements for these certifications.

QUESTION 56

Which role is required to manage groups and policies in Falcon?
* Falcon Host Analyst
* Falcon Host Administrator
* Prevention Hashes Manager
* Falcon Host Security Lead

QUESTION 57

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 58

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 59

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

Explanation

Disabling detections on a host will stop the DetectionSummaryEvent from sending to the Streaming API for that host. This means that the host will not send any detection events to the Streaming API, which is used to stream data from the Falcon Cloud to external applications or systems. The other options are either incorrect or not related to disabling detections on a host. Reference: [CrowdStrike Falcon User Guide], page 32.

QUESTION 60

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

QUESTION 61

Once an exclusion is saved, what can be edited in the future?
* All parts of the exclusion can be changed
* Only the selected groups and hosts to which the exclusion is applied can be changed
* Only the options to “Detect/Block” and/or “File Extraction” can be changed
* The exclusion pattern cannot be changed

QUESTION 62

Which of the follow should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax?
* Sensor Visibility Exclusion
* Machine Learning Exclusions
* IOC Exclusions
* IOA Exclusions

Explanation

The option that should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax is IOA Exclusions. An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. However, using IOA exclusions may reduce the visibility and protection of the Falcon sensor, as it may allow malicious activity to bypass the sensor’s detection and prevention capabilities. Therefore, you should use IOA exclusions with extreme caution and only when necessary2.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 63

Which of the following applies to Custom Blocking Prevention Policy settings?
* Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy
* Blocklisting applies to hashes, IP addresses, and domains
* Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary
* You can only blocklist hashes via the API

QUESTION 64

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?
* Sensor Report
* Machine Learning Prevention Monitoring
* Falcon UI Audit Trail
* Machine Learning Debug

Explanation

The Machine Learning Prevention Monitoring report in the Prevention Policy Management option allows you to monitor the impact of machine learning (ML) prevention settings on your environment. You can view the number of ML detections and preventions by severity, policy, and host group. You can also drill down into specific events and hosts to see more details. This report can help you determine the appropriate ML levels to set in a prevention policy based on your risk tolerance and security posture1.

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

QUESTION 65

Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?
* .*badguydomain.com.*
* DeviceHarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill
* badguydomain.com.*
* Custom IOA rules cannot be created for domains
Explanation

You are usuing RegEx here and need leading “.*” to capture www and then need a “.*” at the end to identify any sites falling under badguydomain.com

QUESTION 66

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?
* ExtendedWindow=1
* Timeout=0
* ProvNoWait=1
* Timeout=30
Explanation

“ProvNoWait=1

The sensor does not abort installation if it can t connect to the CrowdStrike cloud within 20 minutes (10 minutes, in Falcon sensor version 6.21 and earlier). (By default, if the host can’t contact our cloud, it will retry the connection for 20 minutes. After that, the host will automatically uninstall its sensor.)”

“ProvWaitTime=3600000

The sensor waits for 1 hour to connect to the CrowdStrike cloud when installing (the default is 20 minutes).”

QUESTION 67

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

QUESTION 68

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?
* Sensor version set to N-1 and Bulk maintenance mode is turned on
* Sensor version fixed and Uninstall and maintenance protection turned on
* Sensor version updates off and Uninstall and maintenance protection turned off
* Sensor version set to N-2 and Bulk maintenance mode is turned on
Explanation

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from uninstalling or upgrading the sensor, the administrator should set the Sensor version to fixed and turn on the Uninstall and maintenance protection setting in the Sensor Update Policy. This will allow the administrator to specify which sensor version will be used by the hosts using this policy, and also require a maintenance token to uninstall or upgrade the sensor. The other options are either incorrect or not sufficient to meet this criteria. Reference: CrowdStrike Falcon User Guide, page 38.

QUESTION 69

The Customer ID (CID) is important in which of the following scenarios?
* When adding a user to the Falcon console under the Users application
* When performing the sensor installation process
* When setting up API keys
* When performing a Host Search
Explanation

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 70

Which of the following is TRUE of the Logon Activities Report?
* Shows a graphical view of user logon activity and the hosts the user connected to
* The report can be filtered by computer name
* It gives a detailed list of all logon activity for users
* It only gives a summary of the last logon activity for users
Explanation

The Logon Activities Report shows a graphical view of user logon activity and the hosts the user connected to, but it only gives a summary of the last logon activity for users. It does not give a detailed list of all logon activity for users, nor can it be filtered by computer name. The other options are either incorrect or not true of the report. Reference: CrowdStrike Falcon User Guide, page 50.

QUESTION 71

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?
* File exclusions are not aligned to groups or hosts
* There is a limit of three groups of hosts applied to any exclusion
* There is no limit and exclusions can be applied to any or all groups

* Each exclusion can be aligned to only one group of hosts

Explanation

An exclusion is a rule that tells the Falcon platform to ignore certain files, folders, processes, or registry keys when performing prevention or detection actions. An administrator can create an exclusion and apply it to one or more groups of hosts, or to all hosts in the organization. For example, an administrator can create an exclusion for a legitimate application that is causing false positives and apply it to the group of hosts that are running that application.

QUESTION 72

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

* Older versions of the sensor are not available for download
* By emailing CrowdStrike support at support@crowdstrike.com
* By installing the current sensor and clicking the “downgrade” button during the install
* By clicking on “Older versions” links under the Host setup and management > Deploy > Sensor downloads

Explanation

The way to find the older installer file for the Falcon sensor is to click on “Older versions” links under the Host setup and management > Deploy > Sensor downloads. The Sensor downloads page allows you to download the latest version of the Falcon sensor for different operating systems and platforms. However, if you need to install an older version of the sensor, you can click on the “Older versions” links below each sensor download button. This will open a new page where you can select and download any previous version of the sensor1.

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

QUESTION 73

On the Host management page which filter could be used to quickly identify all devices categorized as a

“Workstation” by the Falcon Platform?

* Status
* Platform
* Hostname
* Type

Explanation

The filter that could be used to quickly identify all devices categorized as a “Workstation” by the Falcon Platform on the Host Management page is Type. The Type filter allows you to filter hosts by their device type, such as workstation, server, or domain controller. The device type is assigned to each host based on their Active Directory domain structure. You can use the Type filter to quickly identify all hosts that have the workstation type assigned in their domain2.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 74

How long are detection events kept in Falcon?

* Detection events are kept for 90 days
* Detections events are kept for your subscribed data retention period
* Detection events are kept for 7 days
* Detection events are kept for 30 days

Explanation

” Data is only available in the Falcon UI for investigations, etc. through the company’s data retention time frame; detection information is kept for 90 days regardless; UI audits are available for 1 year

The CCFA-200 certification exam is ideal for IT professionals who are looking to advance their careers in the field of cybersecurity. It is also a great way for individuals who are new to the field to gain the necessary knowledge and skills to start a career in cybersecurity. CrowdStrike Certified Falcon Administrator certification exam is designed to be challenging, but it is also designed to be accessible to individuals with a wide range of experience levels. With the right preparation and dedication, anyone can achieve the CCFA-200 certification and take their career to the next level.

CCFA-200 Dumps - Pass Your Certification Exam:
https://www.testkingfree.com/CrowdStrike/CCFA-200-practice-exam-dumps.html]