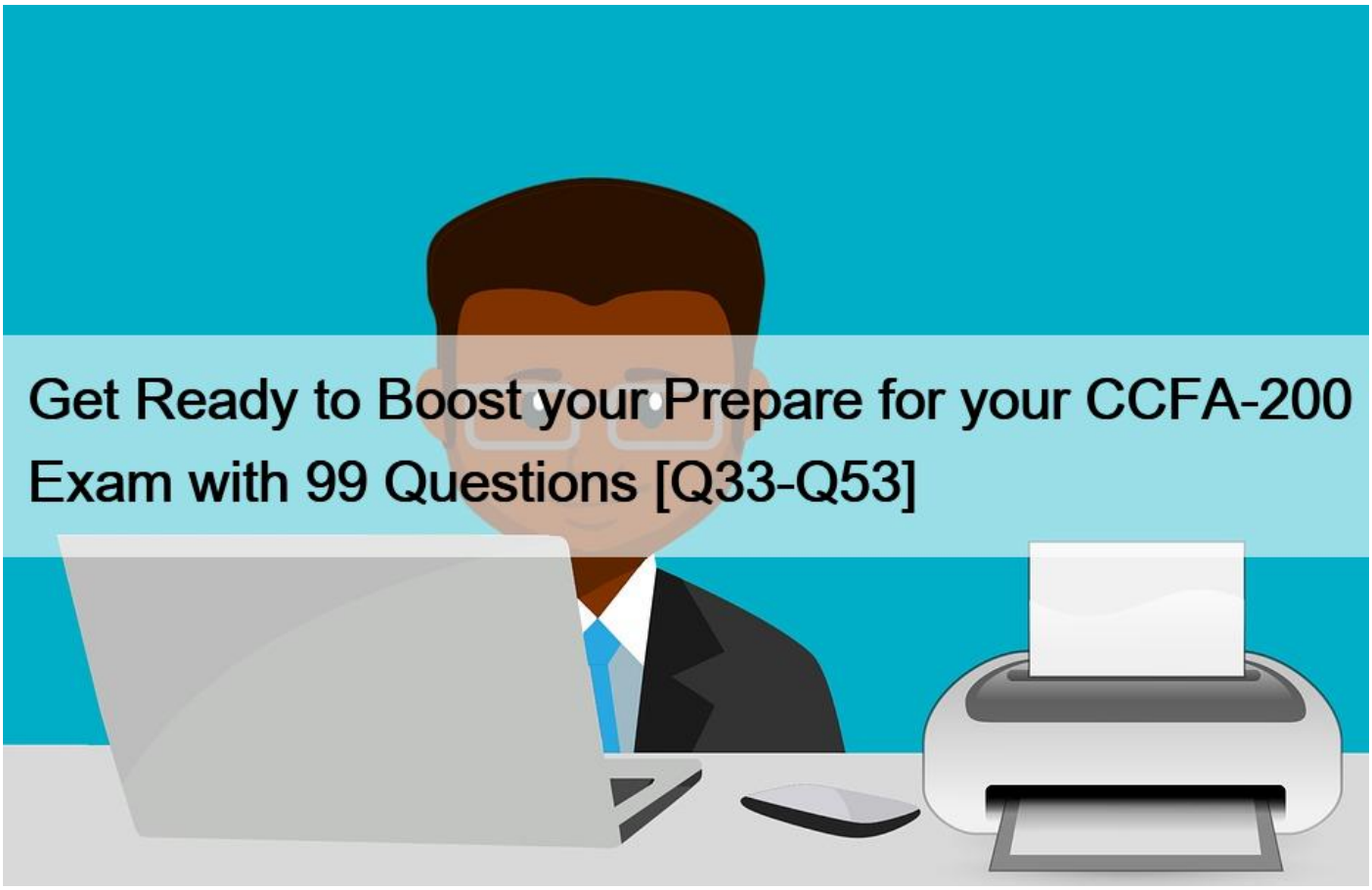
Get Ready to Boost your Prepare for your CCFA-200 Exam with 99 Questions [Q33-Q53



Get Ready to Boost your Prepare for your CCFA-200 Exam with 99 Questions Use Free CCFA-200 Exam Questions that Stimulates Actual EXAM

CrowdStrike CCFA-200 Exam Syllabus Topics:

TopicDetailsTopic 1- Resolve policy settings, permissions and threshold issues- Apply basic sensor install requirements and installation processesTopic 2- Create a new user, delete a user and edit a user, etc- Describe the capabilities and limitations of each RTR roleTopic 3- Explain the differences between the visibility and hunting reports- Explain what information is in the Falcon UI Audit Trail ReportTopic 4- Describe policy types, components, application and workflow- Propose how filtering might be used in the Host Management pageTopic 5- Determine which reports to use when reporting on information relating to a host- Apply appropriate settings to successfully install a Falcon sensor on Windows, Linux and macOSTopic 6- Configure custom alerts to notify individuals about policies, detections and incidents- Recall how long inactive sensors are retained to define your data backup planTopic 7- Perform root cause analysis related to system- user issues- Apply additional - advanced options for images- VDIs, tokens and tagsTopic 8- Explain what information is contained in Machine-Learning Prevention Monitoring Report- Explain the effect of disabling detections on a hostTopic 9- Explain what precedence does regarding prevention policies- Determine roles required for access to features and functionality in the Falcon consoleTopic 10 - Describe what precedence does regarding sensor update policies- Create custom IOA rules to monitor behavior that is not fundamentally maliciousTopic 11- Explain what information can be found in the visibility reports- Explain where build versions are visible for a single sensor or across your environmentTopic 12- Allowlist network traffic so it can connect to

contained hosts- Explain the information shown in the remote logon activity report

NEW QUESTION 33

The alignment of a particular prevention policy to one or more host groups can be completed in which of the following locations within Falcon?
* Policy alignment is configured in the “Host Management” section in the Hosts application
* Policy alignment is configured only once during the initial creation of the policy in the “Create New Policy” pop-up window
* Policy alignment is configured in the General Settings section under the Configuration menu
* Policy alignment is configured in each policy in the “Assigned Host Groups” tab

NEW QUESTION 34

When creating a Host Group for all Workstations in an environment, what is the best method to ensure all workstation hosts are added to the group?
* Create a Dynamic Group with Type=Workstation Assignment
* Create a Dynamic Group and Import All Workstations
* Create a Static Group and Import all Workstations
* Create a Static Group with Type=Workstation Assignment

NEW QUESTION 35

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?
* Edit the Default Response Policy, toggle the “Real Time Response” switch off and assign the policy to the host group
* Edit the Default Response Policy and add the host group to the exceptions list under “Real Time Functionality”
* Create a new Response Policy, toggle the “Real Time Response” switch off and assign the policy to the host group
* Create a new Response Policy and add the host name to the exceptions list under “Real Time Functionality”

NEW QUESTION 36

Which of the following is NOT a way to determine the sensor version installed on a specific endpoint?
* Use the Sensor Report to filter to the specific endpoint
* Use Host Management to select the desired endpoint. The agent version will be listed in the columns and details
* From a command line, run the sc query csagent -version command
* Use the Investigate > Host Search to filter to the specific endpoint

NEW QUESTION 37

How many “Auto” sensor version update options are available for Windows Sensor Update Policies?
* 1
* 2
* 0
* 3

NEW QUESTION 38

Which of the following can a Falcon Administrator edit in an existing user’s profile?
* First or Last name
* Phone number
* Email address
* Working groups

NEW QUESTION 39

The Logon Activities Report includes all of the following information for a particular user EXCEPT _____.
* the account type for the user (e.g. Domain Administrator, Local User)
* all hosts the user logged into
* the logon type (e.g. interactive, service)
* the last time the user’s password was set

NEW QUESTION 40

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

NEW QUESTION 41

How do you disable all detections for a host?
* Create an exclusion rule and apply it to the machine or group of machines
* Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)
* You cannot disable all detections on individual hosts as it would put them at risk
* In Host Management, select the host and then choose the option to Disable Detections

NEW QUESTION 42

When creating new IOCs in IOC management, which of the following fields must be configured?
* Hash, Description, Filename
* Hash, Action and Expiry Date
* Filename, Severity and Expiry Date
* Hash, Platform and Action

NEW QUESTION 43

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?
* Microsoft updates
* Notifications have been disabled on that host sensor
* Falcon console updates are pending
* Falcon sensors installing an update

NEW QUESTION 44

Which of the following Machine Learning (ML) sliders will only detect or prevent high confidence malicious items?
* Aggressive
* Cautious
* Minimal
* Moderate

NEW QUESTION 45

How are user permissions set in Falcon?
* Permissions are token-based. Users request access to a defined set of permissions and an administrator adds their token to the set of permissions
* An administrator selects individual granular permissions from the Falcon Permissions List during user creation
* Permissions are assigned to a User Group and then users are assigned to that group, thereby inheriting those permissions
* Pre-defined permissions are assigned to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments

NEW QUESTION 46

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?
* To group hosts with others in the same business unit
* To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time
* To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion
* To allow the controlled assignment of sensor versions onto specific hosts

NEW QUESTION 47

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

NEW QUESTION 48

What is the primary purpose of using glob syntax in an exclusion?
* To specify a Domain be excluded from detections
* To specify exclusion patterns to easily exclude files and folders and extensions from detections
* To specify exclusion patterns to easily add files and folders and extensions to be prevented
* To specify a network share be excluded from detections

NEW QUESTION 49

On a Windows host, what is the best command to determine if the sensor is currently running?
* sc query csagent
* netstat -a
* This cannot be accomplished with a command
* ping falcon.crowdstrike.com

NEW QUESTION 50

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

NEW QUESTION 51

How does the Unique Hosts Connecting to Countries Map help an administrator?
* It highlights countries with known malware
* It helps visualize global network communication
* It identifies connections containing threats
* It displays intrusions from foreign countries

NEW QUESTION 52

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

NEW QUESTION 53

You have determined that you have numerous Machine Learning detections in your environment that are false positives. They are caused by a single binary that was custom written by a vendor for you and that binary is running on many endpoints. What is the best way to prevent these in the future?
* Contact support and request that they modify the Machine Learning settings to no longer include this detection
* Using IOC Management, add the hash of the binary in question and set the action to “Allow”
* Using IOC Management, add the hash of the binary in question and set the action to “Block, hide detection”
* Using IOC Management, add the hash of the binary in question and set the action to “No Action”