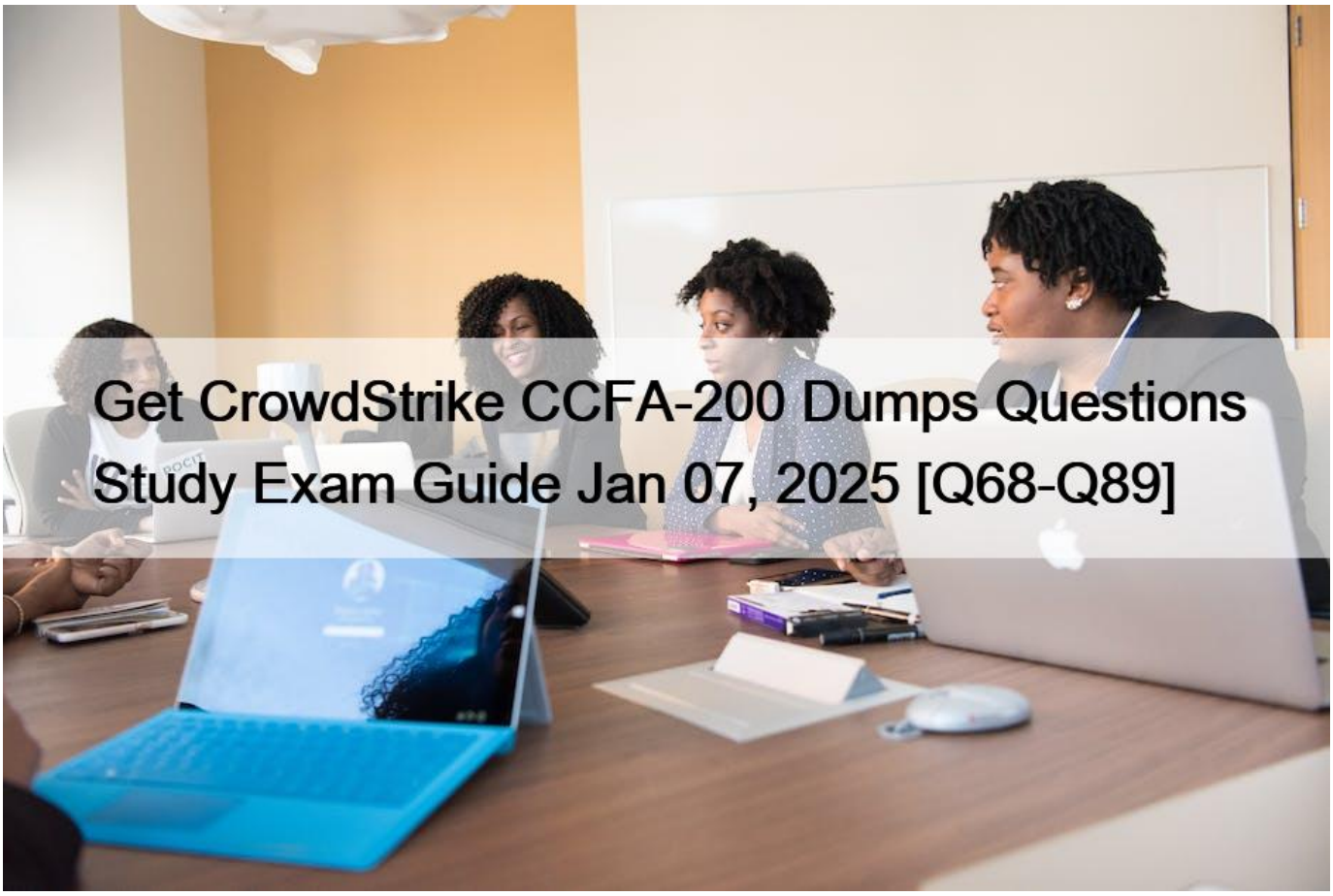
Get CrowdStrike CCFA-200 Dumps Questions Study Exam Guide Jan 07, 2025 [Q68-Q89



Get CrowdStrike CCFA-200 Dumps Questions Study Exam Guide Jan 07, 2025 CCFA-200 Premium Exam Engine - Download Free PDF Questions

The CrowdStrike CCFA-200 exam covers a range of topics, including the fundamentals of Falcon, the installation and configuration of the platform, endpoint management, and incident response. CrowdStrike Certified Falcon Administrator certification exam is based on real-world scenarios that test the candidate's ability to perform tasks related to the administration of Falcon. Upon passing the exam, candidates will receive the CrowdStrike CCFA-200 certification, which demonstrates their proficiency in managing and securing endpoints using Falcon. CrowdStrike Certified Falcon Administrator certification is recognized globally and can help individuals advance their careers in the cybersecurity field.

NO.68 How can you find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days?
* Under Dashboards and reports, choose the Sensor Report. Set the “Last Seen” dropdown to 30 days and reference the Inactive Sensors widget
* Under Host setup and management, choose the Host Management page. Set the group filter to “Inactive Sensors”
* Under Host setup and management > Managed endpoints > Inactive Sensors. Change the time range to 30 days

* Under Host setup and management, choose the Disabled Sensors Report. Change the time range to 30 days

NO.69 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

NO.70 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

NO.71 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

NO.72 With Custom Alerts, it is possible to _____.
* schedule the alert to run at any interval
* receive an alert in an email
* configure prevention actions for alerting
* be alerted to activity in real-time

NO.73 Which of the following prevention policy settings monitors contents of scripts and shells for execution of malicious content on compatible operating systems?
* Script-based Execution Monitoring
* FileSystem Visibility
* Engine (Full Visibility)
* Suspicious Scripts and Commands
Explanation

The prevention policy setting that monitors contents of scripts and shells for execution of malicious content on compatible operating systems is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems.

The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash. You can enable or disable Script-based Execution Monitoring in the Prevention Policy for Windows hosts1.

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

NO.74 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

NO.75 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

NO.76 You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?
* *nix
* Windows
* Both Windows and *nix
* Only Mac

Explanation

A Sensor Update Policy for the Mac platform will only manage Mac operating systems. Sensor Update Policies are platform-specific, meaning that they only apply to hosts that have the same operating system as the policy. For example, a Sensor Update Policy for Windows will only manage Windows hosts, and a Sensor Update Policy for Linux will only manage Linux hosts. You cannot create a Sensor Update Policy that manages multiple operating systems at once2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.77 After Network Containing a host, your Incident Response team states they are unable to remotely connect to the host. Which of the following would need to be configured to allow remote connections from specified IP’s?
* Response Policy
* Containment Policy
* Maintenance Token
* IP Allowlist Management

Explanation

The option that would need to be configured to allow remote connections from specified IP’s after network containing a host is IP Allowlist Management. IP Allowlist Management allows you to define a list of trusted IP addresses that can communicate with your contained hosts. This way, you can isolate a host from the network while still allowing your incident response team or other authorized parties to remotely connect to the host for investigation or remediation purposes2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.78 An analyst has reported they are not receiving workflow triggered notifications in the past few days. Where should you first check for potential failures?
* Custom Alert History
* Workflow Execution log
* Workflow Audit log
* Falcon UI Audit Trail

Explanation

The Workflow Execution log in the Workflow Management option allows you to view the status and results of workflow executions triggered by detection events. You can filter the log by workflow name, status, start and end time, and detection ID. You can also view the details of each execution, including the actions performed, the output received, and any errors encountered. This log can help you troubleshoot potential failures or issues with your workflows1.

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

NO.79 What model is used to create workflows that would allow you to create custom notifications based on particular events which occur in the Falcon platform?
* For – While statement(s)
* Trigger, condition(s) and action(s)
* Event trigger(s)
* Predefined workflow template(s)

NO.80 Which of the following scenarios best describes when you would add IP addresses to the containment policy?
* You want to automate the Network Containment process based on the IP address of a host
* Your organization has additional IP addresses that need to be able to access the Falcon console
* A new group of analysts need to be able to place hosts under Network Containment
* Your organization has resources that need to be accessible when hosts are network contained

Explanation

The scenario that best describes when you would add IP addresses to the containment policy is that your organization has resources that need to be accessible when hosts are network contained. As explained in the previous question, adding IP addresses to the containment policy allows you to create an allowlist of trusted IP addresses that can communicate with your contained hosts. This can be useful when you need to isolate a host from the network due to a potential compromise or investigation, but still want to allow it to access certain resources or services that are essential for your organization’s operations or security2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.81 You need to export a list of all deletions for a specific Host Name in the last 24 hours. What is the best way to do this?
* Go to Host Management in the Host page. Select the host and use the Export Detections button
* Utilize the Detection Resolution Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the “Detection Resolution History” section
* In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results
* Utilize the Detection Activity Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the “Detections by Host” section

NO.82 Which Real Time Response role will allow you to see all analyst session details?
* Real Time Response – Read-Only Analyst
* None of the Real Time Response roles allows this
* Real Time Response -Active Responder
* Real Time Response -Administrator

Explanation

The Real Time Response role that will allow you to see all analyst session details is Real Time Response

-Administrator. A Real Time Response -Administrator is a role that has full access and control over the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. A Real Time Response -Administrator can view all analyst session details, such as session ID, host name, start and end time, commands executed, and output received. A Real Time Response -Administrator can also create, modify, delete, and assign scripts and commands to other analysts2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.83 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

NO.84 When the Notify End Users policy setting is turned on, which of the following is TRUE?
* End users will not be notified as we would not want to notify a malicious actor of a detection. This setting does not exist
* End users will be immediately notified via a pop-up that their machine is in-network isolation
* End-users receive a pop-up notification when a prevention action occurs
* End users will receive a pop-up allowing them to confirm or refuse a pending quarantine

NO.85 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.

NO.86 The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?
* SSL inspection should be configured to occur on all Falcon traffic
* Some network configurations, such as deep packet inspection, interfere with certificate validation
* HTTPS interception should be enabled to proceed with certificate validation
* Common sources of interference with certificate pinning include protocol race conditions and resource contention

NO.87 Why is it important to know your company’s event data retention limits in the Falcon platform?
* This is not necessary; you simply select “All Time” in your query to search all data
* You will not be able to search event data into the past beyond your retention period
* Data such as process records are kept for a shorter time than event data
* Your query will require you to specify the data pool associated with the date you wish to search

Explanation

It is important to know your company’s event data retention limits in the Falcon platform because you will not be able to search event data into the past beyond your retention period. The retention period is the amount of time that event data is stored in the Falcon Cloud, and it may vary depending on your subscription plan and settings. The other options are either incorrect or not related to knowing your retention limits.

Reference: CrowdStrike Falcon User Guide, page 48.

NO.88 Why is the ability to disable detections helpful?
* It gives users the ability to set up hosts to test detections and later remove them from the console
* It gives users the ability to uninstall the sensor from a host
* It gives users the ability to allowlist a false positive detection
* It gives users the ability to remove all data from hosts that have been uninstalled

NO.89 Which is a filter within the Host setup and management > Host management page?
* User name
* OU
* BIOS Version
* Locality

CrowdStrike is a leading provider of cloud-based endpoint security solutions. The company's flagship product, Falcon, is a comprehensive platform that protects organizations from a wide range of cyber threats. CrowdStrike offers certification programs to help IT professionals and security practitioners become proficient in the use of Falcon. The CrowdStrike Certified Falcon Administrator (CCFA-200) exam is one such certification program that is designed to validate an individual's ability to manage and configure Falcon.

Free CCFA-200 Exam Braindumps CrowdStrike Pratice Exam:

https://www.topexamcollection.com/CCFA-200-vce-collection.html]