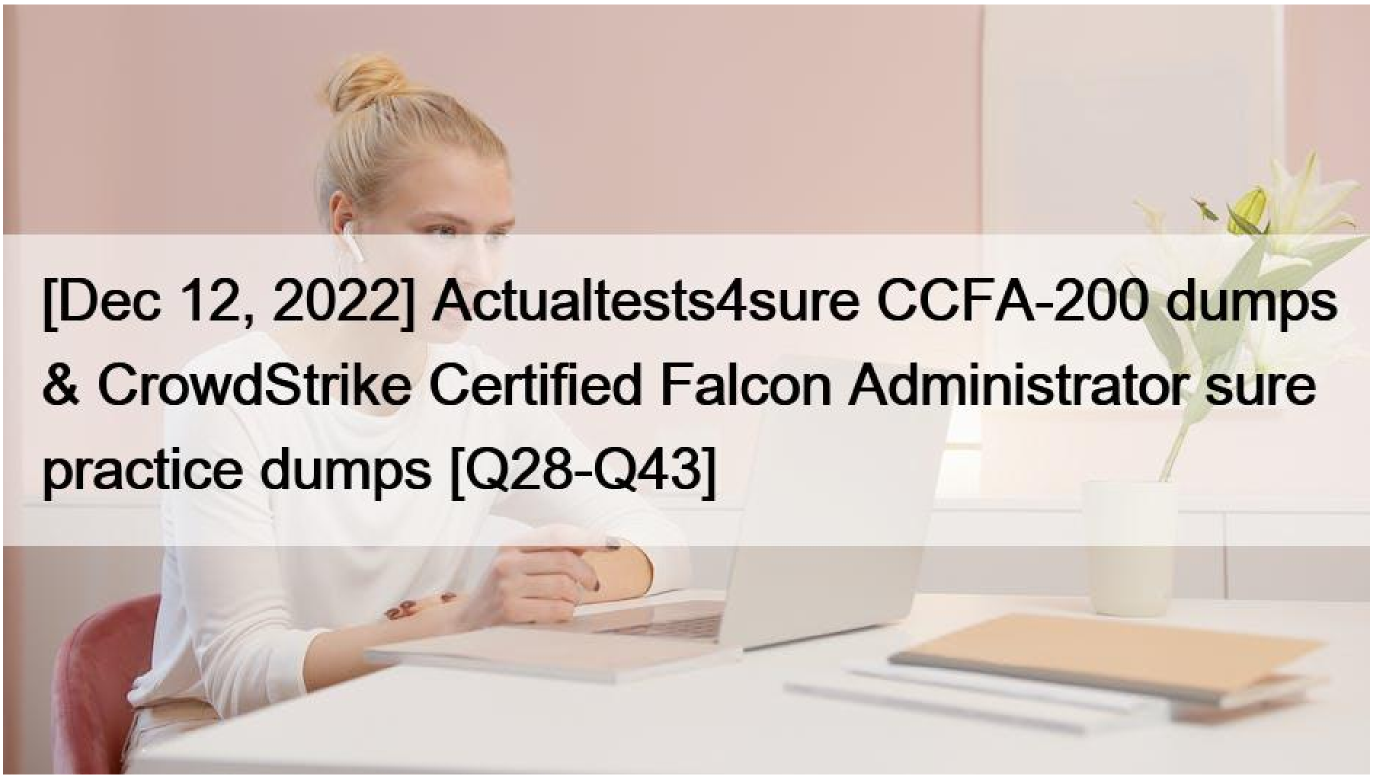
[Dec 12, 2022 Actualtests4sure CCFA-200 dumps & CrowdStrike Certified Falcon Administrator sure practice dumps [Q28-Q43


[Dec 12, 2022] Actualtests4sure CCFA-200 dumps & CrowdStrike Certified Falcon Administrator sure practice dumps [Q28-Q43]

[Dec 12, 2022] Actualtests4sure CCFA-200 dumps & CrowdStrike Certified Falcon Administrator sure practice dumps CrowdStrike CCFA-200 Actual Questions and Braindumps

CrowdStrike CCFA-200 Exam Syllabus Topics:

TopicDetailsTopic 1- Describe policy types, components, application and workflow- Propose how filtering might be used in the Host Management pageTopic 2- 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 3- Explain what Machine Learning is "on sensor" vs. ?the cloud?- Explain the impact of reduced functionality mode (RFM) and why it might be causedTopic 4- Describe what precedence does regarding sensor update policies- Create custom IOA rules to monitor behavior that is not fundamentally maliciousTopic 5- Explain what information can be found in the visibility reports- Explain where build versions are visible for a single sensor or across your environmentTopic 6- Perform root cause analysis related to system- user issues- Apply additional- advanced options for images- VDIs, tokens and tagsTopic 7- Explain what information is contained in Machine-Learning Prevention Monitoring Report- Explain the effect of disabling detections on a hostTopic 8- Resolve policy settings, permissions and threshold issues- Apply basic sensor install requirements and installation processesTopic 9- Create a new user, delete a user and edit a user, etc- Describe the capabilities and limitations of each RTR role

QUESTION 28

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

QUESTION 29

An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?

* The API client secret can be viewed from the Edit API client pop-up box
* Enable the Client Secret column to reveal the API client secret
* Re-create the API client using the exact name to see the API client secret
* The API client secret cannot be retrieved after it has been created

QUESTION 30

Where do you obtain the Windows sensor installer for CrowdStrike Falcon?

* Sensors are downloaded from the Hosts > Sensor Downloads
* Sensor installers are unique to each customer and must be obtained from support
* Sensor installers are downloaded from the Support section of the CrowdStrike website
* Sensor installers are not used because sensors are deployed from within Falcon

QUESTION 31

Which role will allow someone to manage quarantine files?

* Falcon Security Lead
* Detections Exceptions Manager
* Falcon Analyst &#8211; Read Only
* Endpoint Manager

QUESTION 32

What are custom alerts based on?

* Custom workflows
* Custom event based triggers
* Predefined alert templates
* User defined Splunk queries

QUESTION 33

You are evaluating the most appropriate Prevention Policy Machine Learning slider settings for your environment. In your testing phase, you configure the Detection slider as Aggressive. After running the sensor with this configuration for 1 week of testing, which Audit report should you review to determine the best Machine Learning slider settings for your organization?

* Prevention Policy Audit Trail
* Prevention Policy Debug
* Prevention Hashes Ignored
* Machine-Learning Prevention Monitoring

QUESTION 34

Even though you are a Falcon Administrator, you discover you are unable to use the &#8220;Connect to Host&#8221; feature to gather additional information which is only available on the host. Which role do you need added to your user account to have this capability?
* Real Time Responder
* Endpoint Manager
* Falcon Investigator
* Remediation Manager

QUESTION 35

What is the function of a single asterisk (*) in an ML exclusion pattern?
* The single asterisk will match any number of characters, including none. It does include separator characters, such as or /, which separate portions of a file path
* The single asterisk will match any number of characters, including none. It does not include separator characters, such as or /, which separate portions of a file path
* The single asterisk is the insertion point for the variable list that follows the path
* The single asterisk is only used to start an expression, and it represents the drive letter

QUESTION 36

Which role allows a user to connect to hosts using Real-Time Response?
* Endpoint Manager
* Falcon Administrator
* Real Time Responder &#8211; Active Responder
* Prevention Hashes Manager

QUESTION 37

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 &#8220;pop-ups allowed&#8221; in their User Profile configuration page
* By enabling &#8220;Upload quarantined files&#8221; in the General Settings configuration page
* By turning on the &#8220;Notify End Users&#8221; setting at the top of the Prevention policy details configuration page
* By selecting &#8220;Enable pop-up messages&#8221; from the User configuration page

QUESTION 38

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 39

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

QUESTION 40

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

QUESTION 41

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

QUESTION 42

Why is it important to know your company&#8217;s event data retention limits in the Falcon platform?
* This is not necessary; you simply select &#8220;All Time&#8221; 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

QUESTION 43

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase. What settings do you choose?
* Detection slider: Extra Aggressive

Prevention slider: Cautious
* Detection slider: Moderate

Prevention slider: Disabled
* Detection slider: Cautious

Prevention slider: Cautious
* Detection slider: Disabled

Prevention slider: Disabled

Latest CCFA-200 Pass Guaranteed Exam Dumps with Accurate & Updated Questions:
https://www.actualtests4sure.com/CCFA-200-test-questions.html]