[May 27, 2023 CCFA-200 Dumps PDF and Test Engine Exam Questions - BraindumpsIT [Q53-Q77

[May 27, 2023] CCFA-200 Dumps PDF and Test Engine Exam Questions - BraindumpsIT
Verified CCFA-200 exam dumps Q&As with Correct 100 Questions and Answers

QUESTION 53

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 54

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 55

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

QUESTION 56

You want the Falcon Cloud to push out sensor version changes but you also want to manually control when the sensor version is upgraded or downgraded. In the Sensor Update policy, which is the best Sensor version option to achieve these requirements?
* Specific sensor version number
* Auto &#8211; TEST-QA
* Sensor version updates off
* Auto &#8211; N-1

QUESTION 57

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 58

Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?
* Next-Gen Antivirus (NGAV) protection
* Adware and Potentially Unwanted Program detection and prevention
* Real-time offline protection
* Identification and analysis of unknown executables

QUESTION 59

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

QUESTION 60

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

QUESTION 61

What is the purpose of a containment policy?
* To define which Falcon analysts can contain endpoints
* To define the duration of Network Containment
* To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)
* To define allowed IP addresses over which your hosts will communicate when contained

QUESTION 62

You want to create a detection-only policy. How do you set this up in your policy&#8217;s settings?
* Enable the detection sliders and disable the prevention sliders. Then ensure that Next Gen Antivirus is enabled so it will disable Windows Defender.
* Select the &#8220;Detect-Only&#8221; template. Disable hash blocking and exclusions.
* You can&#8217;t create a policy that detects but does not prevent. Use Custom IOA rules to detect.
* Set the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled. Do not activate any of the other blocking or malware prevention options.

QUESTION 63

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?
* There may be special considerations for each OS
* To assist with testing and tracking sensor rollouts
* The network protocols are different for each host OS
* It is an auditing requirement

QUESTION 64

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

QUESTION 65

Which of the following can a Falcon Administrator edit in an existing user&#8217;s profile?
* First or Last name
* Phone number
* Email address
* Working groups

QUESTION 66

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

QUESTION 67

When configuring a specific prevention policy, the admin can align the policy to two different types of groups, Host Groups and which other?
* Custom IOA Rule Groups
* Custom IOC Groups
* Enterprise Groups
* Operating System Groups

QUESTION 68

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

QUESTION 69

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 &#8220;Detection Resolution History&#8221; 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 &#8220;Detections by Host&#8221; section

QUESTION 70

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

QUESTION 71

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

QUESTION 72

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 73

How do you assign a policy to a specific group of hosts?
* Create a group containing the desired hosts using &#8220;Static Assignment.&#8221; Go to the Assigned Host Groups tab of the desired policy and dick &#8220;Add groups to policy.&#8221; Select the desired Group(s).
* Assign a tag to the desired hosts in Host Management. Create a group with an assignment rule based on that tag. Go to the Assignment tab of the desired policy and click &#8220;Add Groups to Policy.&#8221; Select the desired Group(s).
* Create a group containing the desired hosts using &#8220;Dynamic Assignment.&#8221; Go to the Assigned Host Groups tab of the desired policy and select criteria such as OU, OS, Hostname pattern, etc.
* On the Assignment tab of the desired policy, select &#8220;Static&#8221; assignment. From the next window, select the desired hosts (using fitters if needed) and click Add.

QUESTION 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

QUESTION 75

Which option allows you to exclude behavioral detections from the detections page?
* Machine Learning Exclusion
* IOA Exclusion
* IOC Exclusion
* Sensor Visibility Exclusion

QUESTION 76

Under the &#8220;Next-Gen Antivirus: Cloud Machine Learning&#8221; setting there are two categories, one of them is &#8220;Cloud Anti-Malware&#8221; and the other is:
* Adware & PUP
* Advanced Machine Learning
* Sensor Anti-Malware
* Execution Blocking

QUESTION 77

How many &#8220;Auto&#8221; sensor version update options are available for Windows Sensor Update Policies?
* 1
* 2
* 0
* 3

The CrowdStrike CCFA-200 certification is a globally recognized certification that demonstrates an individual's proficiency in managing and securing endpoints using the CrowdStrike Falcon platform. The certification also provides a competitive edge to professionals seeking career advancement opportunities in the cybersecurity industry. Organizations can also benefit from the certification by ensuring that their employees have the necessary skills to manage and secure their endpoints effectively.

CrowdStrike CCFA-200 Test Engine PDF - All Free Dumps: https://www.braindumpsit.com/CCFA-200_real-exam.html]