CrowdStrike.CCFA-200.v2023-05-06.q44

Exam Code:	CCFA-200
Exam Name:	CrowdStrike Certified Falcon Administrator
Certification Provider:	CrowdStrike
Free Question Number:	44
Version:	v2023-05-06
# of views:	749
# of Questions views:	440
https://www.freeqas.com/qa/CrowdStrike/CCFA-200/CrowdStrike.CCFA-200.v2023-05-06.q44.html	

NEW QUESTION: 1
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?
A. Detection slider: Moderate
Prevention slider: Disabled
B. Detection slider: Cautious
Prevention slider: Cautious
C. Detection slider: Disabled
Prevention slider: Disabled
D. Detection slider: Extra Aggressive
Prevention slider: Cautious
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
How many "Auto" sensor version update options are available for Windows Sensor Update Policies?
A. 3
B. 2
C. 1
D. 0
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
Where can you modify settings to permit certain traffic during a containment period?
A. Prevention Policy
B. Containment Policy
C. Firewall Settings

D. Host Settings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
When creating an API client, which of the following must be saved immediately since it cannot be viewed again after the client is created?
A. Client name
B. Secret
C. Base URL
D. Client ID
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
When the Notify End Users policy setting is turned on, which of the following is TRUE?
A. End users will not be notified as we would not want to notify a malicious actor of a detection. This setting does not exist
B. End users will be immediately notified via a pop-up that their machine is in-network isolation
C. End users will receive a pop-up allowing them to confirm or refuse a pending quarantine
D. End-users receive a pop-up notification when a prevention action occurs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
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?
A. Auto - TEST-QA
B. Auto - N-1
C. Specific sensor version number
D. Sensor version updates off
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
You notice there are multiple Windows hosts in Reduced functionality mode (RFM). What is the most likely culprit causing these hosts to be in RFM?
A. A patch was pushed overnight to all Windows systems
B. A Sensor Update Policy was misconfigured
C. A host was placed in network containment from a detection
D. A host was offline for more than 24 hours
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8

How do you assign a policy to a specific group of hosts?
A. Create a group containing the desired hosts using "Dynamic Assignment." Go to the Assigned Host Groups tab of the desired policy and select criteria such as OU, OS, Hostname pattern, etc.
B. Create a group containing the desired hosts using "Static Assignment." Go to the Assigned Host Groups tab of the desired policy and dick "Add groups to policy." Select the desired Group(s).
C. On the Assignment tab of the desired policy, select "Static" assignment. From the next window, select the desired hosts (using fitters if needed) and click Add.
D. 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 "Add Groups to Policy." Select the desired Group(s).
Answer: (SHOW ANSWER)

NEW QUESTION: 9
You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?
A. Windows
B. *nix
C. Only Mac
D. Both Windows and *nix
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
When a host is placed in Network Containment, which of the following is TRUE?
A. The host machine is unable to send or receive network traffic outside of the local network
B. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and any resources allowlisted in the Containment Policy
C. The host machine is unable to send or receive any network traffic
D. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and traffic allowed in the Firewall Policy
Answer: (SHOW ANSWER)

NEW QUESTION: 11
When creating new IOCs in IOC management, which of the following fields must be configured?
A. Hash, Description, Filename
B. Hash, Platform and Action
C. Hash, Action and Expiry Date
D. Filename, Severity and Expiry Date
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
Why would you assign hosts to a static group instead of a dynamic group?

A. You want the group to contain hosts from multiple operating systems
B. You do not want the group membership to change automatically
C. You need hosts to be automatically assigned to a group
D. You are managing more than 1000 hosts
Answer: (SHOW ANSWER)

NEW QUESTION: 13
What information is provided in Logan Activities under Visibility Reports?
A. A list of last endpoints that a user logged in to
B. A list of unique users who are remotely logged on to devices based on the country
C. A list of all logons for all users
D. A list of users who are remotely logged on to devices based on local IP and local port
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What command should be run to verify if a Windows sensor is running?
A. sc query csagent
B. netstat -f
C. regedit myfile.reg
D. ps -ef | grep falcon
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
In order to quarantine files on the host, what prevention policy settings must be enabled?
A. Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration" must be enabled
B. Malware Protection and Windows Anti-Malware Execution Blocking must be enabled
C. Malware Protection and Custom Execution Blocking must be enabled
D. Behavior-Based Threat Prevention sliders and Advanced Remediation Actions must be enabled
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?
A. Microsoft updates
B. Notifications have been disabled on that host sensor
C. Falcon sensors installing an update
D. Falcon console updates are pending
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
When would the No Action option be assigned to a hash in IOC Management?
A. There is no such option as No Action available in the Falcon console
B. Add the indicator to your blocklist and show it as a detection
C. When you want to save the indicator for later action, but do not want to block or allow it at this time
D. Add the indicator to your allowlist and do not detect it
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
Which exclusion pattern will prevent detections on a file at C:\Program Files\My Program\My Files \program.exe?
A. \Program Files\My Program\My Files*
B. *\Program Files\My Program*\
C. **
D. \Program Files\My Program*
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
What must an admin do to reset a user's password?
A. From User Management, select "Reset Password" from the three dot menu for the affected user account
B. From User Management, the administrator must rebuild the account as the certificate for user specific private/public key generation is no longer valid
C. From User Management, open the account details for the affected user and select "Generate New Password"
D. From User Management, select "Update Account" and manually create a new password for the affected user account
Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following is TRUE regarding Falcon Next-Gen AntiVirus (NGAV)?
A. Falcon NGAV is not a replacement for Windows Defender or other antivirus programs

B. Falcon NGAV relies on signature-based detections
C. Activating Falcon NGAV will also enable all detection and prevention settings in the entire policy
D. The Detection sliders cannot be set to a value less aggressive than the Prevention sliders
Answer: (SHOW ANSWER)

NEW QUESTION: 21
An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?
A. The API client secret cannot be retrieved after it has been created
B. Re-create the API client using the exact name to see the API client secret
C. Enable the Client Secret column to reveal the API client secret
D. The API client secret can be viewed from the Edit API client pop-up box
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
One of your development teams is working on code for a new enterprise application but Falcon continually flags the execution as a detection during testing. All development work is required to be stored on a file share in a folder called "devcode." What setting can you use to reduce false positives on this file path?
A. Containment Policy
B. Firewall Rule Group
C. Machine Learning Exclusions
D. USB Device Policy
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Where in the Falcon console can information about supported operating system versions be found?
A. Configuration module
B. Support module
C. Discover module
D. Intelligence module
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which role allows a user to connect to hosts using Real-Time Response?
A. Real Time Responder - Active Responder
B. Endpoint Manager
C. Prevention Hashes Manager
D. Falcon Administrator
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
On a Windows host, what is the best command to determine if the sensor is currently running?
A. This cannot be accomplished with a command
B. ping falcon.crowdstrike.com
C. sc query csagent
D. netstat -a
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
When configuring a specific prevention policy, the admin can align the policy to two different types of groups, Host Groups and which other?
A. Custom IOA Rule Groups
B. Enterprise Groups
C. Operating System Groups
D. Custom IOC Groups
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Under which scenario can Sensor Tags be assigned?
A. While managing hosts in the Falcon console
B. While installing a sensor
C. While triaging a detection
D. While updating a sensor in the Falcon console
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
What is the name for the unique host identifier in Falcon assigned to each sensor during sensor installation?
A. Computer ID (CID)
B. Endpoint ID (EID)
C. Agent ID (AID)
D. Security ID (SID)
Answer: (SHOW ANSWER)

NEW QUESTION: 29
On which page of the Falcon console would you create sensor groups?
A. Sensor update policies
B. Host management
C. Host groups
D. User management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
Which role will allow someone to manage quarantine files?
A. Endpoint Manager
B. Detections Exceptions Manager
C. Falcon Analyst - Read Only
D. Falcon Security Lead
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
What can the Quarantine Manager role do?
A. Manage quarantined files to release and download
B. Manage detection settings
C. Manage roles and users
D. Manage and change prevention settings
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
How do you find a list of inactive sensors?
A. The Falcon platform does not provide reporting for inactive sensors
B. Run the Sensor Aging Report within the Investigate option
C. Run the Inactive Sensor Report in the Host setup and management option
D. A sensor is always considered active until removed by an Administrator
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?
A. TCP port 443 (HTTPS)
B. TCP port 80 (HTTP)
C. TCP UDP port 53 (DNS)
D. TCP port 22 (SSH)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which of the following can a Falcon Administrator edit in an existing user's profile?
A. Email address
B. First or Last name
C. Working groups
D. Phone number
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which is the correct order for manually installing a Falcon Package on a macOS system?
A. Install the Falcon package, then register the Falcon Sensor via command line
B. Register the Falcon Sensor via command line, then install the Falcon package
C. Install the Falcon package, then register the Falcon Sensor via the registration package
D. Register the Falcon Sensor via the registration package, then install the Falcon package
Answer: (SHOW ANSWER)

NEW QUESTION: 36
While a host is Network contained, you need to allow the host to access internal network resources on specific IP addresses to perform patching and remediation. Which configuration would you choose?
A. Configure a Containment Policy with the specific IP addresses
B. Configure the Host firewall to allowlist the specific IP addresses
C. Configure a Containment Policy with the entire internal IP CIDR block
D. Configure a Real Time Response policy allowlist with the specific IP addresses
Answer: (SHOW ANSWER)

NEW QUESTION: 37
What is the maximum number of patterns that can be added when creating a new exclusion?
A. 5
B. 0
C. 10
D. 1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which exclusion pattern will prevent detections on a file at C:\Program Files\My Program\My Files \program.exe?
A. \Program Files\My Program\My Files*
B. \Program Files\My Program*
C. **

D. *\Program Files\My Program*\
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
You have an existing workflow that is triggered on a critical detection that sends an email to the escalation team. Your CISO has asked to also be notified via email with a customized message. What is the best way to update the workflow?
A. Add the CISO's email to the existing action
B. Add a sequential action to send a custom email to your CISO
C. Clone the workflow and replace the existing email with your CISO's email
D. Add a parallel action to send a custom email to your CISO
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
Why is it important to know your company's event data retention limits in the Falcon platform?
A. Your query will require you to specify the data pool associated with the date you wish to search
B. You will not be able to search event data into the past beyond your retention period
C. This is not necessary; you simply select "All Time" in your query to search all data
D. Data such as process records are kept for a shorter time than event data
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?
A. badguydomain\.com.*
B. .*badguydomain.com.*
C. Custom IOA rules cannot be created for domains
D. \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
Which option allows you to exclude behavioral detections from the detections page?
A. IOC Exclusion
B. IOA Exclusion
C. Machine Learning Exclusion
D. Sensor Visibility Exclusion
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
What are custom alerts based on?
A. User defined Splunk queries

B. Custom workflows
C. Predefined alert templates
D. Custom event based triggers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Which role is required to manage groups and policies in Falcon?
A. Falcon Host Administrator
B. Prevention Hashes Manager
C. Falcon Host Security Lead
D. Falcon Host Analyst
Answer: A (LEAVE A REPLY)