CrowdStrike.CCFA-200.v2023-12-02.q61

Exam Code:	CCFA-200
Exam Name:	CrowdStrike Certified Falcon Administrator
Certification Provider:	CrowdStrike
Free Question Number:	61
Version:	v2023-12-02
# of views:	863
# of Questions views:	610
https://www.freepdfdumps.com/CrowdStrike.CCFA-200.v2023-12-02.q61.html	

NEW QUESTION: 1
Which of the following is NOT an available filter on the Hosts Management page?
A. Hostname
B. Username
C. Group
D. OS Version
Answer: B (LEAVE A REPLY)
Explanation
Username is not an available filter on the Hosts Management page. The Hosts Management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions. You can also perform actions such as assigning hosts to groups, updating sensor policies, uninstalling sensors, or isolating hosts1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 2
You have been asked to troubleshoot why Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host. Which report can be used to determine if this is an issue with an old prevention policy?
A. Host Update Status Report
B. Custom Alerting Audit Trail
C. Prevention Policy Debug
D. SBEM Debug Report
Answer: C (LEAVE A REPLY)
Explanation

The report that can be used to determine if Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host due to an old prevention policy is Prevention Policy Debug. The Prevention Policy Debug report allows you to view and compare the prevention policy settings applied to each host in your environment. You can use this report to identify any hosts that have outdated or inconsistent prevention policy settings, such as SBEM, which is a feature that monitors and prevents malicious script execution on Windows systems1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 3
On which page of the Falcon console would you create sensor groups?
A. User management
B. Sensor update policies
C. Host management
D. Host groups
Answer: (SHOW ANSWER)
Explanation
The only place where create host groups is in " Host and setup management > host Groups> Create a group" In Sensor Update policies you can only asign a group of host to the policy not creating a group of hosts.

NEW QUESTION: 4
Where can you find your company's Customer ID (CID)?
A. The CID is a secret key used for Falcon communication and is never shared with the customer
B. The CID is only available by calling support
C. The CID is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the checksum
D. The CID is located at Hosts > Host Management
Answer: (SHOW ANSWER)
Explanation
The CID (Customer ID) is located at Hosts setup and management > Deploy > Sensor Downloads and is listed along with the checksum. The CID is a unique identifier for your organization that is required for authenticating your sensor installation and communication with the Falcon cloud. The checksum is a value that verifies the integrity of the sensor download file. You can find your CID and checksum at the top of the Sensor Downloads page1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 5
Where should you look to find the history of the successes and failures for any Falcon Fusion workflows?

A. Workflow Execution log
B. Falcon UI Audit Trail
C. Workflow Audit log
D. Custom Alert History
Answer: A (LEAVE A REPLY)
Explanation
The place where you can find the history of the successes and failures for any Falcon Fusion workflows is the Workflow Execution log. 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

NEW QUESTION: 6
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?
A. Go to Host Management in the Host page. Select the host and use the Export Detections button
B. 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
C. In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results
D. 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
Answer: C (LEAVE A REPLY)
Explanation
The best way to export a list of all deletions for a specific Host Name in the last 24 hours is to go to the Investigate module, access the Detection Activity page, use the filters to focus on the appropriate hostname and time, then export the results. This will allow you to download a CSV file that contains information about all the detections that were deleted for that host in that time period. The other options are either incorrect or not related to exporting deletions. Reference: CrowdStrike Falcon User Guide, page 49.

NEW QUESTION: 7
How do you assign a Prevention policy to one or more hosts?
A. Create a new policy and assign it directly to those hosts on the Host Management page
B. Modify the users roles on the User Management page
C. Ensure the hosts are in a group and assign that group to a custom Prevention policy
D. Create a new policy and assign it directly to those hosts on the Prevention policy page

Answer: C (LEAVE A REPLY)
Explanation
The administrator can assign a Prevention policy to one or more hosts by ensuring the hosts are in a group and assigning that group to a custom Prevention policy. This allows users to apply different prevention settings and options to different groups of hosts based on their needs and preferences. The other options are either incorrect or not applicable to assigning a Prevention policy. Reference: [CrowdStrike Falcon User Guide], page 34.

NEW QUESTION: 8
If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?
A. Older versions of the sensor are not available for download
B. By emailing CrowdStrike support at support@crowdstrike.com
C. By installing the current sensor and clicking the "downgrade" button during the install
D. By clicking on "Older versions" links under the Host setup and management > Deploy > Sensor downloads
Answer: D (LEAVE A REPLY)
Explanation
The way to find the older installer file for the Falcon sensor is to click on "Older versions" links under the Host setup and management > Deploy > Sensor downloads. The Sensor downloads page allows you to download the latest version of the Falcon sensor for different operating systems and platforms. However, if you need to install an older version of the sensor, you can click on the "Older versions" links below each sensor download button. This will open a new page where you can select and download any previous version of the sensor1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 9
What can exclusions be applied to?
A. Individual hosts selected by the administrator
B. Either all hosts or specified groups
C. Only the default host group
D. Only the groups selected by the administrator
Answer: (SHOW ANSWER)
Explanation
The option that describes what exclusions can be applied to is that exclusions can be applied to either all hosts or specified groups. An exclusion is a rule that defines what files, folders, processes, IP addresses, or domains should be excluded from detection or prevention by the Falcon sensor. You can create and manage exclusions in the Exclusions page in the Falcon console. You can apply exclusions to either all hosts in your

environment or to specific host groups that you select. You cannot apply exclusions to individual hosts selected by the administrator.
References: : [Cybersecurity Resources | CrowdStrike]

NEW QUESTION: 10
Which of the following is TRUE regarding disabling detections for a host?
A. After disabling detections, the host will operate in Reduced Functionality Mode (RFM) until detections are enabled
B. After disabling detections, the data for all existing detections prior to disabling detections is removed from the Event Search
C. The DetectionSummaryEvent continues being sent to the Streaming API for that host
D. The detections for that host are removed from the console immediately. No new detections will display in the console going forward unless detections are enabled
Answer: D (LEAVE A REPLY)
Explanation
The option that is true regarding disabling detections for a host is that the detections for that host are removed from the console immediately. No new detections will display in the console going forward unless detections are enabled. This option is essentially a repetition of question 127 and its answer. Disabling detections for a host will remove any existing detections for that host from the console and prevent any new detections from appearing in the console until detections are enabled again1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 11
What best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page?
A. The detections for the host are removed from the console immediately and no new detections will display in the console going forward
B. You cannot disable detections for a host
C. Existing detections for the host remain, but no new detections will display in the console going forward
D. Preventions will be disabled for the host
Answer: (SHOW ANSWER)
Explanation
The option that best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page is that the detections for the host are removed from the console immediately and no new detections will display in the console going forward. The "Disable 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

NEW QUESTION: 12
What can the Quarantine Manager role do?
A. Manage and change prevention settings
B. Manage quarantined files to release and download
C. Manage detection settings
D. Manage roles and users
Answer: B (LEAVE A REPLY)
Explanation
The Quarantine Manager role can manage quarantined files to release and download. This role allows users to view and search quarantined files, as well as release them from quarantine or download them for further analysis. The other roles do not have this capability. Reference: [CrowdStrike Falcon User Guide], page 19.

NEW QUESTION: 13
You need to have the ability to monitor suspicious VBA macros. Which Sensor Visibility setting should be turned on within the Prevention policy settings?
A. Script-based Execution Monitoring
B. Interpreter-Only
C. Additional User Mode Data
D. Engine (Full Visibility)
Answer: (SHOW ANSWER)
Explanation
Turn on the Script-Based Execution Monitoring prevention policy setting to enable the "Falcon sensor to monitor the contents of scripts and shells that are popular mechanisms for executing malicious code on hosts.
This setting does not kill or block scripts."
Scripting languages:
Excel 4.0 macros
JScript
VBA Macros
VBScript
The Sensor Visibility setting that should be turned on within the Prevention policy settings to monitor suspicious VBA macros 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. VBA (Visual Basic for Applications) is a scripting language that can be embedded in Microsoft Office documents, such as Word or Excel. VBA macros can be used to automate tasks or perform actions within the documents, but they can also be abused by attackers to deliver malware or execute malicious code. Script-based Execution Monitoring can help detect and prevent such attacks by monitoring the contents of VBA macros for execution of malicious content.
References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

NEW QUESTION: 14
Which of the following prevention policy settings monitors contents of scripts and shells for execution of malicious content on compatible operating systems?
A. Script-based Execution Monitoring
B. FileSystem Visibility
C. Engine (Full Visibility)
D. Suspicious Scripts and Commands
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 15
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?
A. Contact support and request that they modify the Machine Learning settings to no longer include this detection
B. Using IOC Management, add the hash of the binary in question and set the action to "Allow"
C. Using IOC Management, add the hash of the binary in question and set the action to "Block, hide detection"
D. Using IOC Management, add the hash of the binary in question and set the action to "No Action"
Answer: (SHOW ANSWER)

Explanation
to match any number of characters including none while not matching beyond path separators (\ or /) and double asterisks are used to recursively match zero or more directories that fall under the current directory.

NEW QUESTION: 16
Why would you assign hosts to a static group instead of a dynamic group?
A. You do not want the group membership to change automatically
B. You are managing more than 1000 hosts
C. You need hosts to be automatically assigned to a group
D. You want the group to contain hosts from multiple operating systems
Answer: A (LEAVE A REPLY)
Explanation
The reason why you would assign hosts to a static group instead of a dynamic group is that you do not want the group membership to change automatically. A Static Group is a group that requires manual assignment or removal of hosts. A Static Group will not update its membership based on any criteria or filters. This way, you can have more control over which hosts belong to the group and prevent any unwanted changes1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 17
Which role allows a user to connect to hosts using Real-Time Response?
A. Endpoint Manager
B. Falcon Administrator
C. Real Time Responder - Active Responder
D. Prevention Hashes Manager
Answer: C (LEAVE A REPLY)
Explanation
The role that allows a user to connect to hosts using Real-Time Response is Real Time Responder - Active Responder. This role allows users to use the "Connect to Host" feature to gather additional information from the host, as well as execute commands and scripts on the host. The other roles do not have this capability.

Reference: [CrowdStrike Falcon User Guide], page 18.

NEW QUESTION: 18
When a host belongs to more than one host group, how is sensor update precedence determined?
A. Groups have no impact on sensor update policies
B. Sensors of hosts that belong to more than one group must be manually updated
C. The highest precedence policy from the most important group is applied to the host
D. All of the host's groups are examined in aggregate and the policy with highest precedence is applied to the host
Answer: D (LEAVE A REPLY)
Explanation
The option that describes how sensor update precedence is determined when a host belongs to more than one host group is that all of the host's groups are examined in aggregate and the policy with highest precedence is applied to the host. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. You can create and assign custom Sensor Update policies to different hosts or groups in your environment. Each Sensor Update policy has a precedence value, which determines its priority over other policies. The higher the precedence value, the higher the priority. If a host belongs to more than one host group, each with a different Sensor Update policy assigned, then all of the host's groups are examined in aggregate and the policy with highest precedence among them is applied to the host.
References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

NEW QUESTION: 19
A sensor that has not contacted the Falcon cloud will be automatically deleted from the hosts list after how many days?
A. 45 Days
B. 60 Days
C. 30 Days
D. 90 Days
Answer: D (LEAVE A REPLY)
Explanation
A sensor that has not contacted the Falcon cloud will be automatically deleted from the hosts list after 90 days.
A sensor that has not contacted the Falcon cloud for more than seven days is considered inactive and will be moved from the Host Management page to the Trash page. An inactive sensor will remain in the Trash page for 90 days before being permanently deleted from the Falcon platform. You can restore an inactive sensor from the Trash page if it contacts the Falcon cloud again within 90 days.
References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

NEW QUESTION: 20
Which of the following is a valid step when troubleshooting sensor installation failure?
A. Confirm all required services are running on the system
B. Enable the Windows firewall
C. Disable SSL and TLS on the host
D. Delete any available application crash log files
Answer: (SHOW ANSWER)
Explanation
A valid step when troubleshooting sensor installation failure is to confirm all required services are running on the system. This can help identify if there are any issues with the sensor service, the Windows Management Instrumentation service, or the Windows Remote Management service, which are required for the sensor to function properly. The other options are either incorrect or not helpful for troubleshooting sensor installation failure. Reference: CrowdStrike Falcon User Guide, page 29.

NEW QUESTION: 21
Which statement is TRUE regarding disabling detections on a host?
A. Hosts with detections disabled will not alert on blocklisted hashes or machine learning detections, but will still alert on IOA-based detections. It will remain that way until detections are enabled again
B. Hosts with detections disabled will not alert on anything until detections are enabled again
C. Hosts with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed
D. Hosts cannot have their detections disabled individually
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 22
Which role is required to manage groups and policies in Falcon?
A. Falcon Host Analyst
B. Falcon Host Administrator

C. Prevention Hashes Manager
D. Falcon Host Security Lead
Answer: (SHOW ANSWER)
Explanation
The Falcon Host Administrator role is required to manage groups and policies in Falcon. This role allows users to create, edit and delete groups and policies, as well as assign them to hosts. The other roles do not have this capability. Reference: [CrowdStrike Falcon User Guide], page 17.

NEW QUESTION: 23
What is the goal of a Network Containment Policy?
A. Increase the aggressiveness of the assigned prevention policy
B. Limit the impact of a compromised host on the network
C. Gain more visibility into network activities
D. Partition a network for privacy
Answer: (SHOW ANSWER)
Explanation
The goal of a Network Containment Policy is to limit the impact of a compromised host on the network. This policy allows users to isolate a host from the network, while still allowing it to communicate with the Falcon Cloud and other essential services. This can help prevent further damage or data exfiltration from a compromised host. The other options are either incorrect or not related to the policy. Reference: [CrowdStrike Falcon User Guide], page 40.

NEW QUESTION: 24
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. Specific sensor version number
B. Auto - TEST-QA
C. Sensor version updates off
D. Auto - N-1
Answer: A (LEAVE A REPLY)
Explanation
The administrator can choose a specific sensor version number in the Sensor Update policy to manually control when the sensor version is upgraded or downgraded. This will allow the Falcon Cloud to push out sensor version changes, but only when the administrator changes the version number in the policy. The other options will either automate the sensor version updates or turn them off completely. Reference: [CrowdStrike Falcon User Guide], page 38.

NEW QUESTION: 25
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?
A. For - While statement(s)
B. Trigger, condition(s) and action(s)
C. Event trigger(s)
D. Predefined workflow template(s)
Answer: B (LEAVE A REPLY)
Explanation
The model that is used to create workflows that would allow you to create custom notifications based on particular events which occur in the Falcon platform is trigger, condition(s) and action(s). This model allows you to specify what event will trigger the workflow, what condition(s) must be met for the workflow to execute, and what action(s) will be performed by the workflow. The other options are either incorrect or not related to creating workflows. Reference: CrowdStrike Falcon User Guide, page 56.

NEW QUESTION: 26
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 traffic allowed in the Firewall 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 any resources allowlisted in the Containment Policy
Answer: (SHOW ANSWER)
Explanation
When a host is placed in Network Containment, 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. This allows users to isolate a host from the network, while still allowing it to communicate with the Falcon Cloud and other essential services. The other options are either incorrect or not true of Network Containment.
Reference: CrowdStrike Falcon User Guide, page 40.

NEW QUESTION: 27
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?
A. ExtendedWindow=1
B. Timeout=0
C. ProvNoWait=1

D. Timeout=30

Answer: C (LEAVE A REPLY)

Explanation

"ProvNoWait=1

The sensor does not abort installation if it can t connect to the CrowdStrike cloud within 20 minutes (10 minutes, in Falcon sensor version 6.21 and earlier). (By default, if the host can't contact our cloud, it will retry the connection for 20 minutes. After that, the host will automatically uninstall its sensor.)"

"ProvWaitTime=3600000

The sensor waits for 1 hour to connect to the CrowdStrike cloud when installing (the default is 20 minutes)."

NEW QUESTION: 28

The Falcon Administrator has created a new prevention policy to apply to the "Servers" group; however, when applying the new prevention policy this group is not appearing in the list of available groups. What is the most likely issue?

A. The new prevention policy should be enabled first

B. The "Servers" group already has a policy applied to it

C. The "Servers" group must be disabled first

D. Host type was not defined correctly within the prevention policy

Answer: B (LEAVE A REPLY)

Explanation

The most likely issue for not being able to apply a new prevention policy to the "Servers" group is that the

"Servers" group already has a policy applied to it. A prevention policy is a policy that defines the prevention capabilities and settings for the Falcon sensor on a host. You can create and assign custom prevention policies to different hosts or groups in your environment. However, you can only assign one prevention policy per host or group at a time. If a host or group already has a prevention policy applied to it, you cannot apply another prevention policy to it unless you remove or replace the existing one2.

References: 2: Cybersecurity Resources | CrowdStrike

NEW QUESTION: 29

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. Base URL

B. Secret

C. Client ID

D. Client name

Answer: B (LEAVE A REPLY)

Explanation

When creating an API client, the secret must be saved immediately since it cannot be viewed again after the client is created. The secret is a randomly generated string that is used to authenticate the API client along with the client ID. The other options are either incorrect or can be viewed or modified later.
Reference: CrowdStrike Falcon User Guide, page 54.

NEW QUESTION: 30
Under which scenario can Sensor Tags be assigned?
A. While triaging a detection
B. While managing hosts in the Falcon console
C. While updating a sensor in the Falcon console
D. While installing a sensor
Answer: (SHOW ANSWER)
Explanation
Check in documentation, there are two kind of tags, the Falcon Grouping Tags that can be managed in falcon console or API and the Sensor Grouping Tags that are configured as parameter in cli, that kind of tags can be diferentiated because it appears with the prefix SensorGroupingTags followed with the name of the tag. If you want to modify a sensor tag is necessary change a registry key value and reboot the device or waiting until the sensor is upgraded.

NEW QUESTION: 31
Why is it important to know your company's event data retention limits in the Falcon platform?
A. This is not necessary; you simply select "All Time" in your query to search all data
B. You will not be able to search event data into the past beyond your retention period
C. Data such as process records are kept for a shorter time than event data
D. Your query will require you to specify the data pool associated with the date you wish to search
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 32
What is the maximum number of patterns that can be added when creating a new exclusion?
A. 10
B. 0
C. 1
D. 5
Answer: C (LEAVE A REPLY)
Explanation
The maximum number of patterns that can be added when creating a new exclusion is one. Each exclusion can only have one pattern, which can be a file path, a hash, a command line or a user name. The other options are either incorrect or not related to creating exclusions. Reference: CrowdStrike Falcon User Guide, page 37.

NEW QUESTION: 33
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. USB Device Policy
B. Firewall Rule Group
C. Containment Policy
D. Machine Learning Exclusions
Answer: D (LEAVE A REPLY)
Explanation
Continment Policy, is a allowlist of IPs and CIDR networks allowed in the moment of a host containtment.
The Machine Learning Exclusions are the way to avoid the detections done it by Machine Learning based on files, so it is possible to exclude the detections for the requested folder with a GLOB expression.

NEW QUESTION: 34

You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?

A. *nix

B. Windows

C. Both Windows and *nix

D. Only Mac

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 35

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

A. File exclusions are not aligned to groups or hosts

B. There is a limit of three groups of hosts applied to any exclusion

C. There is no limit and exclusions can be applied to any or all groups

D. Each exclusion can be aligned to only one group of hosts

Answer: C (LEAVE A REPLY)

Explanation

An exclusion is a rule that tells the Falcon platform to ignore certain files, folders, processes, or registry keys when performing prevention or detection actions. An administrator can create an exclusion and apply it to one or more groups of hosts, or to all hosts in the organization. For example, an administrator can create an exclusion for a legitimate application that is causing false positives and apply it to the group of hosts that are running that application.

NEW QUESTION: 36

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?

A. Falcon console updates are pending

B. Falcon sensors installing an update

C. Notifications have been disabled on that host sensor

D. Microsoft updates

Answer: D (LEAVE A REPLY)

Explanation

The most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM) is Microsoft updates. RFM occurs when the sensor detects a change in the operating system that requires a reboot to complete. Microsoft updates are one of the common causes of such a change. The other options are either incorrect or not related to RFM. Reference: CrowdStrike Falcon User Guide, page 30.

NEW QUESTION: 37
An inactive host that does not contact the Falcon cloud will be automatically removed from the Host Management and Trash pages after how many days?
A. 45 Days
B. 60 Days
C. 75 Days
D. 90 Days
Answer: (SHOW ANSWER)
Explanation
An inactive host that does not contact the Falcon cloud will be automatically removed from the Host Management and Trash pages after 90 days. An inactive host is a host that has not communicated with the Falcon platform for more than seven days. An inactive host will be moved from the Host Management page to the Trash page after seven days of inactivity. An inactive host will remain in the Trash page for 90 days before being permanently deleted from the Falcon platform. You can restore an inactive host from the Trash page if it becomes active again within 90 days1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 38
With Custom Alerts, it is possible to _____.
A. schedule the alert to run at any interval
B. receive an alert in an email
C. configure prevention actions for alerting
D. be alerted to activity in real-time
Answer: B (LEAVE A REPLY)
Explanation
The reporting interval is predefined and cannot be changed. You can only enable/disable the custom alert feature and add/remove recipient email client for the alert/detection.

NEW QUESTION: 39
What would be the most appropriate action to take if you wanted to prevent a folder from being uploaded to the cloud without disabling uploads globally?
A. A Machine Learning exclusion
B. A Sensor Visibility exclusion
C. An IOA exclusion

D. A Custom IOC entry

Answer: D (LEAVE A REPLY)

Explanation

The most appropriate action to take if you wanted to prevent a folder from being uploaded to the cloud without disabling uploads globally is to create a Custom IOC entry. A Custom IOC (indicator of compromise) entry allows you to define custom rules for detecting or preventing malicious activity based on file hashes, file paths, IP addresses, or domains. You can use regex (regular expression) syntax to create a Custom IOC entry that matches the folder path that you want to block from being uploaded to the cloud1.

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

NEW QUESTION: 40

An analyst has reported they are not receiving workflow triggered notifications in the past few days. Where should you first check for potential failures?

A. Custom Alert History

B. Workflow Execution log

C. Workflow Audit log

D. Falcon UI Audit Trail

Answer: (SHOW ANSWER)

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

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. \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill

C. badguydomain\.com.*

D. Custom IOA rules cannot be created for domains

Answer: A (LEAVE A REPLY)

Explanation

You are usuing RegEx here and need leading ".*" to capture www and then need a ".*" at the end to identify any sites falling under badguydomain.com

NEW QUESTION: 42

The Logon Activities Report includes all of the following information for a particular user EXCEPT

_____.

A. the account type for the user (e.g. Domain Administrator, Local User)

B. all hosts the user logged into

C. the logon type (e.g. interactive, service)

D. the last time the user's password was set

Answer: B (LEAVE A REPLY)

Explanation

Checked in console, it returns only the last machine where the user logged on, so it will not return all the machines that the user was logged on in the desired search

NEW QUESTION: 43

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?

A. To group hosts with others in the same business unit

B. To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time

C. To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion

D. To allow the controlled assignment of sensor versions onto specific hosts

Answer: (SHOW ANSWER)

Explanation

The purpose of using groups with Sensor Update policies in CrowdStrike Falcon is to allow the controlled assignment of sensor versions onto specific hosts. This allows users to manage the sensor updates for different hosts based on their needs and preferences, such as testing, staging or production. The other options are either incorrect or not related to using groups with Sensor Update policies. Reference: [CrowdStrike Falcon User Guide], page 38.

NEW QUESTION: 44

What best describes the relationship between Sensor Update policies and Operating Systems?

A. Windows and Mac share Sensor Update policies. Linux requires its own set of polices based on the different kernel versions

B. Sensor Update polices are not Operating System specific. One policy can be applied to all Operating Systems

C. Windows has its own Sensor Update polices. But Mac and Linux share Sensor Update policies

D. A Sensor Update policy must be configured for each Operating System (Windows, Mac, Linux)

Answer: D (LEAVE A REPLY)

Explanation
The option that describes the relationship between Sensor Update policies and Operating Systems is that a Sensor Update policy must be configured for each Operating System (Windows, Mac, Linux). This option is essentially a repetition of question 141 and its answer. Sensor Update policies are specific to each operating system type, as different operating systems have different sensor versions, features, and requirements. Therefore, you need to create and assign separate Sensor Update policies for each operating system type in your environment1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 45
What is the purpose of precedence with respect to the Sensor Update policy?
A. Precedence applies to the Prevention policy and not to the Sensor Update policy
B. Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)
C. Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)
D. Precedence ensures that conflicting policy settings are not set in the same policy
Answer: B (LEAVE A REPLY)
Explanation
The purpose of precedence with respect to the Sensor Update policy is that hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number). This means that if a host belongs to more than one group that has different Sensor Update policies assigned, it will use the policy that has the highest precedence (lowest number) among them. The other options are either incorrect or not related to precedence. Reference: CrowdStrike Falcon User Guide, page 38.

NEW QUESTION: 46
In order to quarantine files on the host, what prevention policy settings must be enabled?
A. Malware Protection and Custom Execution Blocking must be enabled
B. Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration" must be enabled
C. Malware Protection and Windows Anti-Malware Execution Blocking must be enabled
D. Behavior-Based Threat Prevention sliders and Advanced Remediation Actions must be enabled
Answer: B (LEAVE A REPLY)
Explanation
In order to quarantine files on the host, the administrator must enable the Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration" in the prevention policy settings. This will allow Falcon to quarantine malicious files and register

them with Windows Security Center. The other options are either incorrect or not sufficient to enable quarantine. Reference: [CrowdStrike Falcon User Guide], page 36.

NEW QUESTION: 47
Which of the follow should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax?
A. Sensor Visibility Exclusion
B. Machine Learning Exclusions
C. IOC Exclusions
D. IOA Exclusions
Answer: D (LEAVE A REPLY)
Explanation
The option that should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax is IOA Exclusions. An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. However, using IOA exclusions may reduce the visibility and protection of the Falcon sensor, as it may allow malicious activity to bypass the sensor's detection and prevention capabilities. Therefore, you should use IOA exclusions with extreme caution and only when necessary2.
References: 2: Cybersecurity Resources | CrowdStrike

NEW QUESTION: 48
When a Linux host is in Reduced Functionality Mode (RFM) what telemetry and protection is still offered?
A. The sensor would provide protection as normal, without event telemetry
B. The sensor would provide minimal protection
C. The sensor would function as normal
D. The sensor provides no protection, and only collects Sensor Heart Beat events
Answer: (SHOW ANSWER)

Explanation
When a Linux host is in Reduced Functionality Mode (RFM), the sensor would provide minimal protection.
RFM is a mode that limits the sensor's functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Linux sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the /tmp directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud1.
References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NEW QUESTION: 49
Which of the following pages provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System?
A. Support and resources
B. Activity Overview
C. Hosts Overview
D. Sensor Health
Answer: D (LEAVE A REPLY)
Explanation
The page that provides a count of sensors in Reduced Functionality Mode (RFM) by Operating System is Sensor Health. The Sensor Health page allows you to view and monitor the health and status of all sensors in your environment. You can use this page to identify any sensors that have issues or errors, such as RFM, which is a mode that limits the sensor's functionality due to license expiration, network connectivity loss, or certificate validation failure. You can filter the sensors by operating system, sensor version, last seen date, health events, detections, and preventions3.
References: 3: How to Become a CrowdStrike Certified Falcon Administrator

NEW QUESTION: 50
How do you assign a policy to a specific group of hosts?
A. 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).
B. 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).
C. 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.

D. 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.

Answer: (SHOW ANSWER)

Explanation

The administrator can assign a policy to a specific group of hosts by creating a group containing the desired hosts using "Static Assignment." Then, go to the Assigned Host Groups tab of the desired policy and click

"Add groups to policy." Select the desired Group(s). This will apply the policy to the selected group(s) of hosts. The other options are either incorrect or not applicable to static assignment. Reference: [CrowdStrike Falcon User Guide], page 33.

NEW QUESTION: 51

Which of the following applies to Custom Blocking Prevention Policy settings?

A. Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy

B. Blocklisting applies to hashes, IP addresses, and domains

C. Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary

D. You can only blocklist hashes via the API

Answer: A (LEAVE A REPLY)

Explanation

Falcon allows you to upload hashes from your own black or white lists. To enabled this navigate to the Configuration App, Prevention hashes window, and click on "Upload Hashes" in the upper right-hand corner.

Note that you can also automate the task of importing hashes with the CrowdStrike Falcon API.

https://www.crowdstrike.com/blog/tech-center/how-to-prevent-malware-with-custom-blacklisting/

NEW QUESTION: 52

What may prevent a user from logging into Falcon via single sign-on (SSO)?

A. The SSO username doesn't match their email address in Falcon

B. The maintenance token has expired

C. Falcon is in reduced functionality mode

D. The user never configured their security questions

Answer: A (LEAVE A REPLY)

Explanation

The option that may prevent a user from logging into Falcon via single sign-on (SSO) is that the SSO username doesn't match their email address in Falcon. SSO is a feature that allows you to use an external identity provider (IdP) to authenticate and authorize users to

access the Falcon platform. SSO simplifies and streamlines the login process, as users only need to remember one set of credentials for multiple applications.
However, SSO requires that the username in the IdP matches the email address in Falcon for each user. If there is a mismatch between the username and the email address, the user will not be able to log into Falcon via SSO.
References: : [Cybersecurity Resources | CrowdStrike]

NEW QUESTION: 53
Where do you obtain the Windows sensor installer for CrowdStrike Falcon?
A. Sensors are downloaded from the Hosts > Sensor Downloads
B. Sensor installers are unique to each customer and must be obtained from support
C. Sensor installers are downloaded from the Support section of the CrowdStrike website
D. Sensor installers are not used because sensors are deployed from within Falcon
Answer: A (LEAVE A REPLY)
Explanation
The Windows sensor installer for CrowdStrike Falcon can be downloaded from the Hosts > Sensor Downloads page in the Falcon console. This page allows you to download different sensor versions and installers for various operating systems and platforms, as well as view installation instructions and release notes. The other options are either incorrect or not available. Reference: CrowdStrike Falcon User Guide, page 27.

NEW QUESTION: 54
The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?
A. SSL inspection should be configured to occur on all Falcon traffic
B. Some network configurations, such as deep packet inspection, interfere with certificate validation
C. HTTPS interception should be enabled to proceed with certificate validation
D. Common sources of interference with certificate pinning include protocol race conditions and resource contention
Answer: B (LEAVE A REPLY)
Explanation
The statement that some network configurations, such as deep packet inspection, interfere with certificate validation is true concerning Falcon sensor certificate validation. The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks, which means that it verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. Some network configurations, such as deep packet inspection, SSL inspection, or HTTPS interception, may attempt to modify or replace the server certificate, which will cause the sensor to reject the connection and generate an error3.
References: 3: How to Become a CrowdStrike Certified Falcon Administrator

NEW QUESTION: 55
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?
A. Prevention Policy Audit Trail
B. Prevention Policy Debug
C. Prevention Hashes Ignored
D. Machine-Learning Prevention Monitoring
Answer: D (LEAVE A REPLY)
Explanation
Audit logs --> Machine-learning prevention monitoring It shows the count of ML expected detections based on the detection levels for a defined time period and the list of files that would be detected on each detection level.

NEW QUESTION: 56
The alignment of a particular prevention policy to one or more host groups can be completed in which of the following locations within Falcon?
A. Policy alignment is configured in the "Host Management" section in the Hosts application
B. Policy alignment is configured only once during the initial creation of the policy in the "Create New Policy" pop-up window
C. Policy alignment is configured in the General Settings section under the Configuration menu
D. Policy alignment is configured in each policy in the "Assigned Host Groups" tab
Answer: (SHOW ANSWER)
Explanation
The alignment of a particular prevention policy to one or more host groups can be completed in each policy in the "Assigned Host Groups" tab. This tab allows the administrator to select which host groups will use the policy, as well as view the number of hosts and sensors assigned to each group. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 34.

NEW QUESTION: 57
Why is the ability to disable detections helpful?
A. It gives users the ability to set up hosts to test detections and later remove them from the console
B. It gives users the ability to uninstall the sensor from a host
C. It gives users the ability to allowlist a false positive detection

D. It gives users the ability to remove all data from hosts that have been uninstalled
Answer: (SHOW ANSWER)
Explanation
"Disable Detections. This is helpful for users who want to set up hosts to test detections in the Falcon console and who later want to remove those old test detections from the"

NEW QUESTION: 58
What best describes what happens to detections in the console after clicking "Enable Detections" for a host which previously had its detections disabled?
A. Enables custom detections for the host
B. New detections will start appearing in the console, and all retroactive stored detections will be restored to the console for that host
C. New detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host
D. Preventions will be enabled for the host
Answer: (SHOW ANSWER)
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

NEW QUESTION: 59
How long are detection events kept in Falcon?
A. Detection events are kept for 90 days
B. Detections events are kept for your subscribed data retention period
C. Detection events are kept for 7 days
D. Detection events are kept for 30 days
Answer: A (LEAVE A REPLY)
Explanation
" Data is only available in the Falcon UI for investigations, etc. through the company's data retention time frame; detection information is kept for 90 days regardless; UI audits are available for 1 year

NEW QUESTION: 60
To enhance your security, you want to detect and block based on a list of domains and IP addresses. How can you use IOC management to help this objective?
A. Blocking of Domains and IP addresses is not a function of IOC management. A Custom IOA Rule should be used instead
B. Using IOC management, import the list of hashes and IP addresses and set the action to Detect Only
C. Using IOC management, import the list of hashes and IP addresses and set the action to Prevent/Block
D. Using IOC management, import the list of hashes and IP addresses and set the action to No Action
Answer: A (LEAVE A REPLY)
Explanation
IOC management only allows "Detect only" and "No Action" among the possible actions. Therefore, it cannot be used to block based on IPs or domains. Custom IOA Rule groups allow to create rule types based on Network Connection (configuring a remote IP address) and domains, and gives the options to "Monitor",
"Detect" and "Kill Process", being the late one the closest to "block".

NEW QUESTION: 61
When uninstalling a sensor, which of the following is required if the 'Uninstall and maintenance protection' setting is enabled within the Sensor Update Policies?
A. Maintenance token
B. Customer ID (CID)
C. Bulk update key
D. Agent ID (AID)
Answer: A (LEAVE A REPLY)
Explanation
When uninstalling a sensor, a maintenance token is required if the 'Uninstall and maintenance protection' setting is enabled within the Sensor Update Policies. This setting prevents unauthorized or accidental uninstallation of sensors by requiring a token that can be generated from the Falcon console. The other options are either incorrect or not related to uninstalling a sensor. Reference: CrowdStrike Falcon User Guide, page
29.

here: https://www.actual4test.com/CCFA-200_examcollection.html (**152** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

Valid CCFA-200 Dumps shared by Actual4test.com for Helping Passing CCFA-200 Exam! Actual4test.com now offer the **newest CCFA-200 exam dumps**, the Actual4test.com CCFA-200 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCFA-200 dumps with Test Engine here: https://www.actual4test.com/CCFA-200_examcollection.html (**152** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)