ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

What is the function of a single asterisk (*) in an ML exclusion pattern?

A. 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
B. 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
C. The single asterisk is the insertion point for the variable list that follows the path
D. The single asterisk is only used to start an expression, and it represents the drive letter

Answer: B

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/machine-learning

The asterisk is a wildcard character that can be used in exclusion patterns to match any number of characters. However, it does not match separator characters, such as \ or /, which are used to separate portions of a file path. For example, the pattern C:\Windows**.exe will match any executable file in any subfolder of the Windows folder, but not in the Windows folder itself.
Reference: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 2

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: B

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.

Question: 3

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints

B. To define the duration of Network Containment

C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)

D. To define allowed IP addresses over which your hosts will communicate when contained

Answer: D

Explanation:

In the Containment Policy page have the title "Network traffic allowlist" and it only allows to add IPs or CIDR networks to exclude in the moment of the isolation of any host, because it is a global policy, not allowing make distinctions between machines.

Question: 4

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

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.
Reference: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 5

Even though you are a Falcon Administrator, you discover you are unable to use the "Connect to Host" 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?

A. Real Time Responder
B. Endpoint Manager
C. Falcon Investigator
D. Remediation Manager

Answer: A

Explanation:

The Real Time Responder role allows users to use the “Connect to Host” feature to gather additional information from the host, such as running processes, registry keys, files, etc. The other roles do not have this capability.
Reference: CrowdStrike Falcon User Guide, page 18.

Question: 6

What must an admin do to reset a user's password?

A. From User Management, open the account details for the affected user and select "Generate New Password"
B. From User Management, select "Reset Password" from the three dot menu for the affected user account
C. From User Management, select "Update Account" and manually create a new password for the affected user account
D. From User Management, the administrator must rebuild the account as the certificate for user specific private/public key generation is no longer valid

Answer: B

Explanation:

The administrator can reset a user's password by selecting "Reset Password" from the three dot menu for the affected user account in the User Management page. This will generate a new password and send it to the user's email address. The other options are either incorrect or not available. Reference: CrowdStrike Falcon User Guide, page 25.

Question: 7

Your organization has a set of servers that are not allowed to be accessed remotely, including via Real Time Response (RTR). You already have these servers in their own Falcon host group. What is the next step to disable RTR only on these hosts?

A. Edit the Default Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group
B. Edit the Default Response Policy and add the host group to the exceptions list under "Real Time Functionality"
C. Create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group
D. Create a new Response Policy and add the host name to the exceptions list under "Real Time Functionality"

Answer: C

Explanation:

The administrator can create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group that contains the servers that are not allowed to be accessed remotely. This will disable RTR only on those hosts, while keeping it enabled for the rest of the hosts. Editing the Default Response Policy or adding exceptions will not achieve the desired result. Reference: CrowdStrike Falcon User Guide, page 35.

Question: 8

When creating new IOCs in IOC management, which of the following fields must be configured?

A. Hash, Description, Filename
B. Hash, Action and Expiry Date
C. Filename, Severity and Expiry Date
D. Hash, Platform and Action

Answer: D

Explanation:

When creating new IOCs in IOC management, the administrator must configure the Hash, Platform and Action fields. The Hash field is the value of the IOC, such as MD5, SHA1 or SHA256. The Platform field is the operating system that the IOC applies to, such as Windows, Linux or Mac. The Action field is the action that Falcon will take when detecting the IOC, such as Detect, Block or Allow. The other fields are either optional or not available. Reference: CrowdStrike Falcon User Guide, page 44

Question: 9

Your CISO has decided all Falcon Analysts should also have the ability to view files and file contents locally on compromised hosts, but without the ability to take them off the host. What is the most appropriate role that can be added to fullfil this requirement?

A. Remediation Manager
B. Real Time Responder – Read Only Analyst
C. Falcon Analyst – Read Only
D. Real Time Responder – Active Responder

Answer: B

Explanation:

The Real Time Responder - Read Only Analyst only allows to run the commands "cat,cd,clear,env,eventlog,filehash,getsid,help,history,ipconfig,ls,mount,netstat,ps,reg" the role do not have permission to get files so it is the most aproximated profile for the requested capabilities.

Question: 10

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

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.

Question: 11

How do you disable all detections for a host?

A. Create an exclusion rule and apply it to the machine or group of machines

B. Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)

C. You cannot disable all detections on individual hosts as it would put them at risk

D. In Host Management, select the host and then choose the option to Disable Detections

Answer: D

Explanation:

The administrator can disable all detections for a host by selecting the host and then choosing the option to Disable Detections in the Host Management page. This will prevent the host from sending any detection events to the Falcon Cloud. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 32.

Question: 12

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

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".

Question: 13

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: B

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.

Question: 14

Which of the following can a Falcon Administrator edit in an existing user's profile?

A. First or Last name
B. Phone number
C. Email address
D. Working groups

Answer: A

Explanation:

Roles are never called 'working groups' in the documentation. The only other option that can be edited on a existing user is first and last name.

Question: 15

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

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.

Question: 16

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: B

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.

Question: 17

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

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/

Question: 18

How many "Auto" sensor version update options are available for Windows Sensor Update Policies?

A. 1
B. 2
C. 0

D. 3

Answer: D

Explanation:

There are three “Auto” sensor version update options available for Windows Sensor Update Policies: Auto - N-1, Auto - TEST-QA and Auto - Latest. These options allow the administrator to automatically update the sensor version to the previous stable version, the latest test version or the latest stable version, respectively. Reference: [CrowdStrike Falcon User Guide], page 38.

Question: 19

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: D

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.

Question: 20

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

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

Question: 21

What information is provided in Logan Activities under Visibility Reports?

A. A list of all logons for all users
B. A list of last endpoints that a user logged in to
C. A list of users who are remotely logged on to devices based on local IP and local port
D. A list of unique users who are remotely logged on to devices based on the country

Answer: B

Explanation:

The Logon Activities report under Visibility Reports provides a list of last endpoints that a user logged in to. This report shows the user name, domain name, logon type, logon time and endpoint name for each logon event. The other options are either incorrect or not related to the report. Reference: [CrowdStrike Falcon User Guide], page 50.

Question: 22

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

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.

Question: 23

What command should be run to verify if a Windows sensor is running?

A. regedit myfile.reg
B. sc query csagent
C. netstat -f
D. ps -ef | grep falcon

Answer: B

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.

Question: 24

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. Custom IOC Groups
C. Enterprise Groups
D. Operating System Groups

Answer: A

Explanation:

Prevention Policies are created based on the OS (Windows, MAC and Linux policies). Once a prevention policy is created, three options appear on top: Settings, Assigned Host Groups and Assigned Custom IOAS (tested on Crowdstrike). Therefore, Host Groups and Custom IOAS are the two different types of groups a prevention policy can be aligned to.

Question: 25

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

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.

Question: 26

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

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)."

Question: 27

How can you find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days?

A. Under Dashboards and reports, choose the Sensor Report. Set the "Last Seen" dropdown to 30 days and reference the Inactive Sensors widget
B. Under Host setup and management, choose the Host Management page. Set the group filter to "Inactive Sensors"
C. Under Host setup and management > Managed endpoints > Inactive Sensors. Change the time range to 30 days
D. Under Host setup and management, choose the Disabled Sensors Report. Change the time range to 30 days

Answer: C

Explanation:

The administrator can find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days by going to Host setup and management > Managed endpoints > Inactive Sensors. Then, change the time range to 30 days. This will show the host name, last seen date, sensor version and group name for each inactive host. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 31.

Question: 28

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

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.

Question: 29

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

A. There may be special considerations for each OS
B. To assist with testing and tracking sensor rollouts
C. The network protocols are different for each host OS
D. It is an auditing requirement

Answer: A

Explanation:

https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/

Question: 30

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: A

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.

Question: 31

You want to create a detection-only policy. How do you set this up in your policy's settings?

A. Enable the detection sliders and disable the prevention sliders. Then ensure that Next Gen Antivirus is enabled so it will disable Windows Defender.
B. Select the "Detect-Only" template. Disable hash blocking and exclusions.
C. You can't create a policy that detects but does not prevent. Use Custom IOA rules to detect.
D. 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.

Answer: D

Explanation:

The administrator can create a detection-only policy by setting the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled in the policy's settings. This will allow Falcon to detect but not prevent threats on the hosts using this policy. Do not activate any of the other blocking or malware prevention options, as they will enable prevention actions. The other options are either incorrect or not related to creating a detection-only policy. Reference: [CrowdStrike Falcon User Guide], page 35.

Question: 32

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

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

Question: 33

Where can you modify settings to permit certain traffic during a containment period?

A. Prevention Policy
B. Host Settings
C. Containment Policy
D. Firewall Settings

Answer: C

Explanation:

The administrator can modify settings to permit certain traffic during a containment period by creating or editing a Containment Policy. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment. Reference: [CrowdStrike Falcon User Guide], page 40.

Question: 34

Which option allows you to exclude behavioral detections from the detections page?

A. Machine Learning Exclusion
B. IOA Exclusion
C. IOC Exclusion
D. Sensor Visibility Exclusion

Answer: B

Explanation:

IOA Exclusion says - Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection. Source: https://falcon.crowdstrike.com/documentation/68/detection-and-prevention-policies#exclusions

Question: 35

What are custom alerts based on?

A. Custom workflows
B. Custom event based triggers
C. Predefined alert templates
D. User defined Splunk queries

Answer: C

Explanation:

Scheduling a Custom Alert for your environment consists of three steps: choosing the template you'd like to configure, previewing the search results, then scheduling the alert. Use Custom Alerts to configure email alerts using predefined templates so you're notified about specific activity in your environment. When an alert runs and finds results, it sends an email to specified recipients instead of generating a new detection. Custom Alerts let you set up email alerts based on predefined templates that cover a wide range of topics including Real Time Response session initiation, host containment, OS security settings, and more that are not yet covered by notification workflows.

Question: 36

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

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.

Question: 37

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 Sensor Update Policy was misconfigured
B. A host was ofline for more than 24 hours
C. A patch was pushed overnight to all Windows systems
D. A host was placed in network containment from a detection

Answer: C

Explanation:

The most likely culprit causing multiple Windows hosts to be in Reduced Functionality Mode (RFM) is a patch that was pushed overnight to all Windows systems. RFM occurs when the sensor detects a change in the operating system that requires a reboot to complete. A patch is 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.

Question: 38

Which of the following is TRUE of the Logon Activities Report?

A. Shows a graphical view of user logon activity and the hosts the user connected to
B. The report can be filtered by computer name
C. It gives a detailed list of all logon activity for users
D. It only gives a summary of the last logon activity for users

Answer: D

Explanation:

The Logon Activities Report shows a graphical view of user logon activity and the hosts the user connected to, but it only gives a summary of the last logon activity for users. It does not give a detailed list of all logon activity for users, nor can it be filtered by computer name. The other options are either incorrect or not true of the report. Reference: CrowdStrike Falcon User Guide, page 50.

Question: 39

Which of the following roles allows a Falcon user to create Real Time Response Custom Scripts?

A. Real Time Responder – Administrator
B. Real Time Responder – Read Only Analyst
C. Real Time Responder – Script Developer
D. Real Time Responder – Active Responder

Answer: A

Explanation:

Real Time Responder - Administrator (RTR Administrator) - Can do everything RTR Active Responder can do, plus create custom scripts, upload files to hosts using the put command, and directly run executables using the run command.

Question: 40

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

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.

Question: 41

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

Answer: D

Explanation:

The API client secret cannot be retrieved after it has been created. The secret is only displayed once when the API client is created, and it cannot be viewed or edited later. Therefore, it is important to save the secret securely and use it along with the client ID to authenticate the API client. The other options are either incorrect or not possible. Reference: CrowdStrike Falcon User Guide, page 54.

Question: 42

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?

A. TCP port 22 (SSH)
B. TCP port 443 (HTTPS)
C. TCP port 80 (HTTP)
D. TCP UDP port 53 (DNS)

Answer: B

Explanation:

The sensor uses TCP port 443 (HTTPS) to communicate with the CrowdStrike Cloud. This port and protocol are used to securely send and receive data between the sensor and the cloud, such as detections, policies, updates, commands, etc. The other options are either incorrect or not used by the sensor. Reference: CrowdStrike Falcon User Guide, page 28.

Question: 43

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

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.

Question: 44

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

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.

Question: 45

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: D

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.

Question: 46

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 Real Time Response policy allowlist with the specific IP addresses
B. Configure a Containment Policy with the specific IP addresses
C. Configure a Containment Policy with the entire internal IP CIDR block

D. Configure the Host firewall to allowlist the specific IP addresses

Answer: B

Explanation:

While a host is Network contained, the administrator can allow the host to access internal network resources on specific IP addresses to perform patching and remediation by configuring a Containment Policy with the specific IP addresses. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment. Reference: [CrowdStrike Falcon User Guide], page 40.

Question: 47

Which of the following is TRUE regarding Falcon Next-Gen AntiVirus (NGAV)?

A. Falcon NGAV relies on signature-based detections
B. Activating Falcon NGAV will also enable all detection and prevention settings in the entire policy
C. The Detection sliders cannot be set to a value less aggressive than the Prevention sliders
D. Falcon NGAV is not a replacement for Windows Defender or other antivirus programs

Answer: C

Explanation:

The Detection sliders cannot be set to a value less aggressive than the Prevention sliders in Falcon Next-Gen AntiVirus (NGAV). This is because prevention is a subset of detection, and it would not make sense to prevent threats that are not detected. The other options are either incorrect or not true of Falcon NGAV. Reference: [CrowdStrike Falcon User Guide], page 35.

Question: 48

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: D

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.

Question: 49

What impact does disabling detections on a host have on an API?

A. Endpoints with detections disabled will not alert on anything until detections are enabled again
B. Endpoints cannot have their detections disabled individually
C. DetectionSummaryEvent stops sending to the Streaming API for that host
D. Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

Answer: C

Explanation:

Disabling detections on a host will stop the DetectionSummaryEvent from sending to the Streaming API for that host. This means that the host will not send any detection events to the Streaming API, which is used to stream data from the Falcon Cloud to external applications or systems. The other options are either incorrect or not related to disabling detections on a host. Reference: [CrowdStrike Falcon User Guide], page 32.

Question: 50

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: D

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.

Question: 51

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell
C. Yara
D. Regex

Answer: D

Explanation:

Regex guidelines https://falcon.crowdstrike.com/documentation/68/detection-and-prevention-policies#regex

Question: 52

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

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.

Question: 53

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

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.

Question: 54

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are

not allowed to run in your environment. You have chosen to use Falcon to do this. Which is the best way to accomplish this?

A. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running

B. Using Custom Alerts in the Investigate App, create a new alert using the template "Process Execution" and within that rule, select the option to "Block Execution"

C. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.

D. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"

Answer: C

Explanation:

The best way to ensure that a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers are not allowed to run in your environment is to use IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking. This will allow Falcon to block the execution of these hashes on the hosts using this policy. The other options are either incorrect or not efficient to achieve this goal. Reference: [CrowdStrike Falcon User Guide], page 44.

Question: 55

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

Explanation:

The exclusion pattern that will prevent detections on a file at C:\Program Files\My Program\My

Files\program.exe is \Program Files\My Program\My Files*. This pattern will match any file under the My Files folder, including program.exe, and exclude them from detections. The other patterns are either incorrect or too broad to prevent detections on this specific file. Reference: [CrowdStrike Falcon User Guide], page 37.

Question: 56

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: D

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.

Question: 57

When would the No Action option be assigned to a hash in IOC Management?

A. When you want to save the indicator for later action, but do not want to block or allow it at this time
B. Add the indicator to your allowlist and do not detect it
C. There is no such option as No Action available in the Falcon console
D. Add the indicator to your blocklist and show it as a detection

Answer: A

Explanation:

The No Action option can be assigned to a hash in IOC Management when you want to save the indicator for later action, but do not want to block or allow it at this time. This option will neither detect nor prevent the execution of the hash, but will keep it in the IOC list for future reference. The other options are either incorrect or not related to the No Action option. Reference: CrowdStrike Falcon User Guide, page 44.

Question: 58

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

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.

Question: 59

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

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.

Question: 60

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

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.

Question: 61

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?

A. By ensuring each user has set the "pop-ups allowed" in their User Profile configuration page
B. By enabling "Upload quarantined files" in the General Settings configuration page
C. By turning on the "Notify End Users" setting at the top of the Prevention policy details configuration page
D. By selecting "Enable pop-up messages" from the User configuration page

Answer: C

Explanation:

A Falcon Administrator can configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity by turning on the “Notify End Users” setting at the top of the Prevention policy details configuration page. This setting allows users to enable or disable end user notifications for prevention actions taken by Falcon on Windows hosts. The other options are either incorrect or not related to configuring pop-up messages. Reference: CrowdStrike Falcon User Guide, page 36.

Question: 62

Where in the Falcon console can information about supported operating system versions be found?

A. Configuration module
B. Intelligence module
C. Support module
D. Discover module

Answer: C

Explanation:

Information about supported operating system versions can be found in the Support module in the Falcon console. This module provides access to various support resources, such as documentation, downloads, FAQs, release notes and system status. One of the documents available in this module is the CrowdStrike Sensor Compatibility List, which lists the supported operating system versions for each sensor type and platform. The other options are either incorrect or not related to finding information about supported operating system versions. Reference: CrowdStrike Falcon User Guide,

page 26.

Question: 63

What is the name for the unique host identifier in Falcon assigned to each sensor during sensor installation?

A. Endpoint ID (EID)
B. Agent ID (AID)
C. Security ID (SID)
D. Computer ID (CID)

Answer: B

Explanation:

The name for the unique host identifier in Falcon assigned to each sensor during sensor installation is Agent ID (AID). The AID is a 32-character hexadecimal string that uniquely identifies each sensor and host in the Falcon platform. The other options are either incorrect or not related to the sensor identifier. Reference: CrowdStrike Falcon User Guide, page 28.

Question: 64

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: A

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.

Question: 65

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

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.

Question: 66

Which role will allow someone to manage quarantine files?

A. Falcon Security Lead
B. Detections Exceptions Manager
C. Falcon Analyst – Read Only
D. Endpoint Manager

Answer: A

Explanation:

The role that will allow someone to manage quarantine files is Falcon Security Lead. This role allows users to view and manage 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.

Question: 67

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

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.

Question: 68

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

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.

Question: 69

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?

A. Sensor version set to N-1 and Bulk maintenance mode is turned on
B. Sensor version fixed and Uninstall and maintenance protection turned on
C. Sensor version updates off and Uninstall and maintenance protection turned off
D. Sensor version set to N-2 and Bulk maintenance mode is turned on

Answer: B

Explanation:

In order to exercise manual control over the sensor upgrade process, as well as prevent unauthorized users from uninstalling or upgrading the sensor, the administrator should set the Sensor version to fixed and turn on the Uninstall and maintenance protection setting in the Sensor Update Policy. This will allow the administrator to specify which sensor version will be used by the hosts using this policy, and also require a maintenance token to uninstall or upgrade the sensor. The other options are either incorrect or not sufficient to meet this criteria. Reference: CrowdStrike Falcon User Guide, page 38.

Question: 70

Once an exclusion is saved, what can be edited in the future?

A. All parts of the exclusion can be changed
B. Only the selected groups and hosts to which the exclusion is applied can be changed
C. Only the options to "Detect/Block" and/or "File Extraction" can be changed

D. The exclusion pattern cannot be changed

Answer: A

Explanation:

Once an exclusion is saved, all parts of the exclusion can be changed in the future. The administrator can edit an existing exclusion by selecting it from the Exclusions page and modifying any of its fields, such as pattern, type, option, group or host. The other options are either incorrect or not true of editing exclusions. Reference: CrowdStrike Falcon User Guide, page 37.

Question: 71

Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?

A. Next-Gen Antivirus (NGAV) protection
B. Adware and Potentially Unwanted Program detection and prevention
C. Real-time ofline protection
D. Identification and analysis of unknown executables

Answer: D

Explanation:

According to documentation (documentation/detections/technique/sensor-based-ml-cst0007): CrowdStrike sensor-based machine learning (ML) identifies and analyzes unknown executables as they run on hosts. This technique is triggered by files and file attributes associated with known malware. This is similar to the [Cloud-based ML](/support/documentation/detections/technique/cloud-based-ml) technique. Cloud-based ML is informed by global analysis of executables that classifies and identifies malware. The key difference is that it doesn't run on hosts when they're ofline.

Question: 72

How do you find a list of inactive sensors?

A. The Falcon platform does not provide reporting for inactive sensors
B. A sensor is always considered active until removed by an Administrator
C. Run the Inactive Sensor Report in the Host setup and management option
D. Run the Sensor Aging Report within the Investigate option

Answer: C

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 73

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?

A. Sensor Report
B. Machine Learning Prevention Monitoring
C. Falcon UI Audit Trail
D. Machine Learning Debug

Answer: B

Explanation:

The Machine Learning Prevention Monitoring report in the Prevention Policy Management option allows you to monitor the impact of machine learning (ML) prevention settings on your environment. You can view the number of ML detections and preventions by severity, policy, and host group. You can also drill down into specific events and hosts to see more details. This report can help you determine the appropriate ML levels to set in a prevention policy based on your risk tolerance and security posture1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 74

Why is the ability to disable detections helpful?

A. It gives usersthe ability to set up hosts to test detections and laterremove them from the console
B. It gives usersthe ability to uninstall the sensor from a host
C. It gives usersthe ability to allowlist a false positive detection
D. It gives usersthe ability to remove all data from hosts that have beenuninstalled

Answer: A

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"

Question: 75

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

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

Question: 76

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: B

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 77

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. Clone the workflow and replace the existing email with your CISO's email
B. Add a sequential action to send a custom email to your CISO
C. Add a parallel action to send a custom email to your CISO
D. Add the CISO's email to the existing action

Answer: C

Explanation:

The best way to update the workflow is to add a parallel action to send a custom email to your CISO. A parallel action allows you to perform multiple actions simultaneously when a workflow is triggered, without affecting the order or outcome of other actions. A sequential action, on the other

hand, requires one action to complete before another action can start. By adding a parallel action, you can ensure that both the escalation team and your CISO receive an email notification as soon as possible1.

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

Question: 78

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

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.

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

Question: 79

What is the primary purpose of using glob syntax in an exclusion?

A. To specify a Domain be excluded from detections
B. To specify exclusion patterns to easily exclude files and folders and extensions from detections
C. To specify exclusion patterns to easily add files and folders and extensions to be prevented
D. To specify a network share be excluded from detections

Answer: B

Explanation:

Glob syntax is used to specify exclusion patterns to easily exclude files and folders and extensions from detections. Glob syntax allows you to use wildcards (*) and ranges ([a-z]) to match multiple characters or values in a file path or name. For example, you can use glob syntax to exclude all files with .exe extension in a folder by using C:\Folder*.exe as an exclusion pattern2.

Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 80

How are user permissions set in Falcon?

A. Permissions are assigned to a User Group and then users are assigned to that group,

thereby

inheriting those permissions

B. Pre-defined permissions are assigned to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments C. An administrator selects individual granular permissions from the Falcon Permissions List during user creation

D. Permissions are token-based. Users request access to a defined set of permissions and an administrator adds their token to the set of permissions

Answer: B

Explanation:

User permissions are set in Falcon by assigning pre-defined permissions to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments. Roles are collections of permissions that define what users can see and do in Falcon. Permissions are granular actions that allow users to access specific features or functions in Falcon. For example, a user who is assigned both the Falcon Administrator role and the Falcon Investigator role will have all the permissions from both roles2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 81

Which of the following is NOT a way to determine the sensor version installed on a specific endpoint?

A. Use the Sensor Report to filter to the specific endpoint
B. Use the Investigate > Host Search to filter to the specific endpoint
C. Use Host Management to select the desired endpoint. The agent version will be listed in the columns and details
D. From a command line, run the sc query csagent -version command

Answer: D

Explanation:

From a command line, running the sc query csagent -version command is not a way to determine the sensor version installed on a specific endpoint. This command will only show the status of the csagent service, not the sensor version. The other options are valid ways to determine the sensor version installed on a specific endpoint using Falcon UI or API. You can use the Sensor Report, the Host Search, or the Host Management features to filter, search, or select the desired endpoint and view the sensor version information12.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike 2: How to Become a CrowdStrike Certified Falcon Administrator

Question: 82

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 the registration package
B. Install the Falcon package, then register the Falcon Sensor via command line
C. Register the Falcon Sensor via command line, then install the Falcon package
D. Register the Falcon Sensor via the registration package, then install the Falcon package

Answer: B

Explanation:

The correct order for manually installing a Falcon Package on a macOS system is to install the Falcon package, then register the Falcon Sensor via command line. The Falcon package contains the sensor binary and the kernel extension, while the registration package contains the customer ID and the sensor group ID. The registration package is not required for macOS systems, as the registration information can be provided via command line after installing the Falcon package1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 83

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: Extra Aggressive
Prevention slider: Cautious
B.
Detection slider: Moderate
Prevention slider: Disabled
C.
Detection slider: Cautious
Prevention slider: Cautious
D.
Detection slider: Disabled
Prevention slider: Disabled

Answer: C

Explanation:
The best settings to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase are Cautious for both Detection and Prevention sliders. This setting will enable the sensor to detect and prevent only high-confidence malicious events, while allowing low-confidence events to run without interference. This setting will also generate less noise and false positives than higher settings, such as Moderate or Extra Aggressive1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 84

How does the Unique Hosts Connecting to Countries Map help an administrator?

A. It highlights countries with known malware
B. It helps visualize global network communication
C. It identifies connections containing threats

D. It displays intrusions from foreign countries

Answer: B

Explanation:

The Unique Hosts Connecting to Countries Map helps an administrator to visualize global network communication. The map shows the number of unique hosts in your environment that have established network connections to different countries in the past 24 hours. You can use this map to identify unusual or suspicious network activity, such as connections to high-risk countries or regions, or connections from hosts that are not expected to communicate with external entities2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 85

On a Windows host, what is the best command to determine if the sensor is currently running?

A. sc query csagent
B. netstat -a
C. This cannot be accomplished with a command
D. ping falcon.crowdstrike.com

Answer: A

Explanation:

On a Windows host, the best command to determine if the sensor is currently running is sc query csagent. This command will show the status of the csagent service, which is responsible for running the sensor on Windows systems. The output of this command will indicate if the service is running, stopped, or paused. If the service is running, the sensor is also running3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 86

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

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.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 87

Which is a filter within the Host setup and management > Host management page?

A. User name
B. OU
C. BIOS Version
D. Locality

Answer: B

Explanation:

OU (organizational unit) is a filter within the Host setup and management > Host management page. The Host 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 filter by OU, which is a logical grouping of hosts based on their Active Directory domain structure1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 88

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?

A. Create a Dynamic Group with Type=Workstation Assignment
B. Create a Dynamic Group and Import All Workstations
C. Create a Static Group and Import all Workstations
D. Create a Static Group with Type=Workstation Assignment

Answer: A

Explanation:

The best method to ensure all workstation hosts are added to the group is to create a Dynamic Group with Type=Workstation Assignment. A Dynamic Group is a group that automatically updates its membership based on certain criteria or filters. A Type=Workstation Assignment filter will match all hosts that have the workstation type assigned in their Active Directory domain. This way, any new or existing workstation hosts will be added to the group without manual intervention1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 89

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 receive a pop-up notification when a prevention action occurs
D. End users will receive a pop-up allowing them to confirm or refuse a pending quarantine

Answer: C

Explanation:

When the Notify End Users policy setting is turned on, end-users receive a pop-up notification when a prevention action occurs. This setting allows you to inform the end-users that the Falcon sensor has blocked or quarantined a malicious item on their system. The notification will also provide the name and path of the item, the reason for the prevention, and a link to contact support if needed1.

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

Question: 90

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

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.

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

Question: 91

Which of the following best describes the Default Sensor Update policy?

A. The Default Sensor Update policy does not have the "Uninstall and maintenance protection" feature
B. The Default Sensor Update policy is only used for testing sensor updates
C. The Default Sensor Update policy is a "catch-all" policy
D. The Default Sensor Update policy is disabled by default

Answer: C

Explanation:

The Default Sensor Update policy is a “catch-all” policy. This means that any host that is not assigned to a specific sensor update policy will inherit the settings from the Default Sensor Update policy. The Default Sensor Update policy is enabled by default and has the “Uninstall and maintenance protection” feature turned on. You can modify the settings of the Default Sensor Update policy, but you cannot delete or disable it2.

Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 92

Under the "Next-Gen Antivirus: Cloud Machine Learning" setting there are two categories, one of them is "Cloud Anti-Malware" and the other is:

A. Adware & PUP
B. Advanced Machine Learning
C. Sensor Anti-Malware
D. Execution Blocking

Answer: A

Explanation:

With EDR license, if you go to "Audit logs > Machine-learning prevention monitoring", three options appear: Cloud Anti-malware, Sensor Anti-malware and Adware&PUP. Therefore, answer is A.

Question: 93

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

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.

Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 94

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

A. Aggressive
B. Cautious
C. Minimal
D. Moderate

Answer: B

Explanation:

The Machine Learning (ML) slider that will only detect or prevent high confidence malicious items is Cautious. The ML slider allows you to adjust the level of sensitivity and aggressiveness of the Falcon sensor's ML engine, which uses artificial intelligence to identify and stop unknown threats. The Cautious setting will enable the sensor to detect and prevent only high-confidence malicious events, while allowing low-confidence events to run without interference. This setting will also generate less noise and false positives than higher settings, such as Moderate or Extra Aggressive1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 95

What type of information is found in the Linux Sensors Dashboard?

A. Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage
B. Hidden File execution, Execution of file from the trash, Versions Running with Computer Names
C. Versions running, Directory Made Invisible to Spotlight, Logging/Auditing Referenced, Viewed, or Modified
D. Private Information Accessed, Archiving Tools – Exfil, Files Made Executable

Answer: A

Explanation:

The type of information that is found in the Linux Sensors Dashboard is Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage. The Linux Sensors Dashboard is a dashboard that provides an overview of the Linux hosts in your environment that have Falcon sensors installed. You can use this dashboard to monitor the health and activity of your Linux hosts, such as their kernel versions, root shell usage, network communication, detections, and preventions3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 96

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

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 97

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

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 98

Which of the following uses Regex to create a detection or take a preventative action?

A. Custom IOC
B. Machine Learning Exclusion
C. Custom IOA
D. Sensor Visibility Exclusion

Answer: C

Explanation:

The option that uses regex to create a detection or take a preventative action is Custom IOA.
A

Custom IOA (indicator of attack) allows you to define custom rules for detecting or preventing suspicious behavior based on process execution, file write, network connection, or registry events. You can use regex syntax to create a Custom IOA rule that matches the event data that you want to monitor or block1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 99

When creating a custom IOA for a specific domain, which syntax would be best for detecting or preventing on all subdomains as well?

A. *\.baddomain\.xyz|baddomain\. xyz
B. *baddomain\. xyz|baddomain\. xyz. *
C. Custom IOA rules cannot be created for domains
D. **baddomain\. xyz|baddomain\. xyz**

Answer: A

Explanation:

The syntax that would be best for detecting or preventing on all subdomains as well is *.baddomain.xyz|baddomain. xyz. This syntax will match any domain that ends with .baddomain.xyz or is exactly baddomain.xyz. The * wildcard will match any characters before the dot, and the | operator will match either side of the expression. This syntax can be used in a Custom IOC or a Custom IOA rule to detect or prevent network connections to malicious domains1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 100

What statement is TRUE about managing a user's role?

A. The Administrator cannot re-use the account email for a new account
B. You must have Falcon MFA enabled first
C. You must be a Falcon Security Lead
D. You must be a Falcon Administrator

Answer: D

Explanation:

The statement that is true about managing a user's role is that you must be a Falcon Administrator. A Falcon Administrator is a role that has full access and control over all features and functions in Falcon, including user management. A Falcon Administrator can create, modify, delete, and assign roles to other users in Falcon. A Falcon Administrator can also re-use the account email for a new account, enable Falcon MFA (multi-factor authentication), and assign other roles such as Falcon Security Lead or Falcon Investigator2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 101

Which Real Time Response role will allow you to see all analyst session details?

A. Real Time Response - Read-Only Analyst
B. None of the Real Time Response roles allows this
C. Real Time Response -Active Responder
D. Real Time Response -Administrator

Answer: D

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.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 102

Which command would tell you if a Falcon Sensor was running on a Windows host?

A. cswindiag.exe -status
B. netstat.exe -f
C. sc.exe query csagent
D. sc.exe query falcon

Answer: C

Explanation:

The command that would tell you if a Falcon Sensor was running on a Windows host is sc.exe query csagent. This command will show the status of the csagent service, which is responsible for running the sensor on Windows systems. The output of this command will indicate if the service is running, stopped, or paused. If the service is running, the sensor is also running3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 103

On which page of the Falcon console can one locate the Customer ID (CID)?

A. Hosts Management

B. API Clients and Keys

C. Sensor Dashboard
D. Sensor Downloads

Answer: B

Explanation:

The page of the Falcon console where one can locate the Customer ID (CID) is API Clients and Keys. The API Clients and Keys page allows you to create and manage API clients and keys for accessing the Falcon platform programmatically. The Customer ID (CID) is a unique identifier for your organization that is required for authenticating your API requests. You can find your CID at the top of the API Clients and Keys page2.

Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 104

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?

A. Response Policy
B. Containment Policy
C. Maintenance Token
D. IP Allowlist Management

Answer: D

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.

Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 105

Which of the following controls the speed in which your sensors will receive automatic sensor updates?

A. Maintenance Tokens
B. Sensor Update Policy
C. Sensor Update Throttling
D. Channel File Update Throttling

Answer: C

Explanation:

The option that controls the speed in which your sensors will receive automatic sensor updates

is Sensor Update Throttling. Sensor Update Throttling allows you to limit the number of sensors that can download a new sensor version per hour. This way, you can avoid network congestion or bandwidth issues caused by simultaneous sensor updates. You can configure the Sensor Update Throttling setting in the Sensor Update Policy for each platform1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 106

Which of the following tools developed by Crowdstrike is intended to help with removal of the CrowdStrike Windows Falcon Sensor?

A. CrowdStrikeRemovalTool.exe
B. UninstallTool.exe
C. CSUninstallTool.exe
D. FalconUninstall.exe

Answer: C

Explanation:

The tool developed by Crowdstrike that is intended to help with removal of the CrowdStrike Windows Falcon Sensor is CSUninstallTool.exe. This tool is a command-line utility that can uninstall the Falcon sensor from a Windows system without requiring user interaction or network connectivity. The tool can also bypass the Uninstall and Maintenance Protection feature if enabled in the Sensor Update Policy2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 107

When a user initiates a sensor installs, where can the logs be found?

A. %SYSTEMROOT%\Logs
B. %SYSTEMROOT%\Temp
C. %LOCALAPPDATA%\Logs
D. % LOCALAPP D ATA%\Tem p

Answer: B

Explanation:

When a user initiates a sensor install, the logs can be found in %SYSTEMROOT%\Temp. This folder contains temporary files and folders created by the system or applications, including the sensor installation logs. The sensor installation logs have names that start with CSFalconContainer and end with .log, such as CSFalconContainer-2023-08-31_11-23-21.log. These logs can help you troubleshoot any issues or errors that may occur during the sensor installation process3.

Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 108

After agent installation, an agent opens a permanent connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated.

A. SSH
B. TLS
C. HTTP
D. TCP

Answer: B

Explanation:

After agent installation, an agent opens a permanent TLS connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated. TLS (Transport Layer Security) is a protocol that provides secure and encrypted communication between the agent and the Falcon cloud. Port 443 is the standard port for HTTPS (Hypertext Transfer Protocol Secure) traffic. The agent uses this connection to send and receive data, commands, policies, and updates from the Falcon cloud2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 109

Which of the following best describes what the Uninstall and Maintenance Protection setting controls within your Sensor Update Policy?

A. Prevents automatic updates of the sensor
B. Prevents the sensor from entering Reduced Functionality Mode
C. Prevents modification of sensor update policy
D. Prevents unauthorized uninstallation of the sensor

Answer: D

Explanation:

The option that best describes what the Uninstall and Maintenance Protection setting controls within your Sensor Update Policy is that it prevents unauthorized uninstallation of the sensor. The Uninstall and Maintenance Protection setting is a feature that adds an extra layer of security to the sensor by requiring a maintenance token to uninstall or update the sensor manually. The maintenance token is a unique code that can be generated by a Falcon Administrator or a Real Time Response - Administrator in the Falcon console. Without a valid maintenance token, the sensor cannot be uninstalled or updated by anyone, including local administrators or malware2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 110

Which option best describes the general process Whereinstallation of the Falcon Sensor on MacOS?

A. Grant the Falcon Package Full Disk Access, install the Falcon package, use falconctl to license the sensor

B. Install the Falcon package passing it the installation token in the command line

C. Install the Falcon package, use falconctl to license the sensor, approve the system extension, grant the sensor Full Disk Access

D. Grant the Falcon Package Full Disk Access, install the Falcon package, load the Falcon Sensor with the command 'falconctl stats'

Answer: C

Explanation:

The option that best describes the general process for installation of the Falcon Sensor on MacOS is to install the Falcon package, use falconctl to license the sensor, approve the system extension, grant the sensor Full Disk Access. The Falcon package contains the sensor binary and the kernel extension, which can be installed by double-clicking on it or using a command-line tool such as installer. The falconctl tool is a command-line utility that allows you to configure and manage the sensor on MacOS systems. You can use falconctl to license the sensor by providing your Customer ID (CID) and optionally your Sensor Group ID (SGID). After licensing the sensor, you need to approve the system extension in the Security & Privacy settings of your system preferences, which will require a restart. Finally, you need to grant the sensor Full Disk Access in the Privacy settings of your system preferences, which will allow the sensor to monitor and protect your files and folders1.

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

Question: 111

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: C

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.

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

Question: 112

A Falcon Administrator is trying to use Real-Time Response to start a session with a host that has a sensor installed but they are unable to connect. What is the most likely cause?

A. The host has a user logged into it
B. The domain controller is preventing the connection
C. They do not have an RTR role assigned to them
D. There is another analyst connected into it

Answer: C

Explanation:

The most likely cause for not being able to use Real-Time Response to start a session with a host that has a sensor installed is that they do not have an RTR role assigned to them. An RTR (Real Time Response) role is a role that grants access and permissions to use the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. There are three types of RTR roles: Real Time Response -Read-Only Analyst, Real Time Response -Active Responder, and Real Time Response -Administrator. You need to have at least one of these roles assigned to you in order to use Real Time Response2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 113

What should be disabled on firewalls so that the sensor's man-in-the-middle attack protection works properly?

A. Deep packet inspection
B. Linux Sub-System
C. PowerShell
D. Windows Proxy

Answer: A

Explanation:

The option that should be disabled on firewalls so that the sensor's man-in-the-middle attack protection works properly is deep packet inspection. Deep packet inspection is a network configuration that inspects and modifies the data packets that pass through a firewall. Deep packet inspection may interfere with the sensor's certificate validation, which is a feature that verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. If the certificate validation fails, the sensor will reject the connection and generate an error3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 114

When troubleshooting the Falcon Sensor on Windows, what is the correct parameter to output the log directory to a specified file?

A. LOG=log.txt
B. \log log.txt
C. C:\CSSensorInstall\LogFiles
D. /log log.txt

Answer: D

Explanation:

The correct parameter to output the log directory to a specified file when troubleshooting the Falcon Sensor on Windows is /log log.txt. This parameter will create a log file named log.txt in the same folder where you run the sensor installation command. The log file will contain information about the sensor installation process, such as the parameters used, the actions performed, and any errors encountered3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 115

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

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 116

What information does the API Audit Trail Report provide?

A. A list of analyst login activity
B. A list of specific changes to prevention policy
C. A list of actions taken via Falcon OAuth2-based APIs
D. A list of newly added hosts

Answer: C

Explanation:

The information that the API Audit Trail Report provides is a list of actions taken via Falcon OAuth2- based APIs. The API Audit Trail Report allows you to view and audit the activity and

usage of the Falcon APIs by different API clients and users in your organization. You can use this report to monitor who accessed what data, when, and how via the Falcon APIs2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 117

What three things does a workflow condition consist of?

A. A parameter, an operator, and a value
B. A beginning, a middle, and an end
C. Triggers, actions, and alerts
D. Notifications, alerts, and API's

Answer: A

Explanation:

A workflow condition consists of a parameter, an operator, and a value. A workflow condition is a rule that defines when a workflow should be triggered based on certain criteria or filters. A parameter is a variable or attribute that can be used to filter or match detection events, such as severity, tactic, or host group. An operator is a symbol or word that specifies how to compare or evaluate the parameter and the value, such as equals, contains, or greater than. A value is a constant or expression that provides the expected or desired result for the parameter, such as high, credential dumping, or default group1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 118

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

A. Workflow Execution log
B. Falcon Ul Audit Trail
C. Workflow Audit log
D. Custom Alert History

Answer: A

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 119

A. Enable Behavior-Based Threat Prevention sliders and Advanced Remediation Actions
B. Enable Malware Protection and Windows Anti-Malware Execution Blocking
C. Enable Next-Gen Antivirus Prevention sliders and "Quarantine & Security Center Registration
D. Enable Malware Protection and Custom Execution Blocking

Answer: C

Explanation:

The option that will enable Next-Gen Antivirus Prevention sliders and “Quarantine & Security Center Registration” is to enable Malware Protection and Windows Anti-Malware Execution Blocking. Malware Protection is a feature that enables the Next-Gen Antivirus Prevention sliders, which allow you to adjust the level of sensitivity and aggressiveness of the Falcon sensor’s machine learning engine, which uses artificial intelligence to identify and stop unknown threats. Windows Anti-Malware Execution Blocking is a feature that enables the “Quarantine & Security Center Registration” setting, which allows you to quarantine malicious files and register them in the Windows Security Center1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 120

You have a new patch server that should be reachable while hosts in your environment are network contained. The server's IP address is static and does not change. Which of the following is the best approach to updating the Containment Policy to allow this?

A. Add an allowlist entry for the individual server's MAC address
B. Add an allowlist entry containing the host group that the server belongs to
C. Add an allowlist entry for the individual server's IP address
D. Add an allowlist entry containing CIDR notation for the /24 network the server belongs to

Answer: C

Explanation:

The best approach to updating the Containment Policy to allow a new patch server that should be reachable while hosts in your environment are network contained is to add an allowlist entry for the individual server’s IP address. An allowlist entry 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 it to access essential resources or services, such as a patch server. If the server’s IP address is static and does not change, adding an individual IP address is more precise and secure than adding a host group or a network range2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 121

Which of the following scenarios best describes when you would add IP addresses to the

containment policy?

A. You want to automate the Network Containment process based on the IP address of a host
B. Your organization has additional IP addresses that need to be able to access the Falcon console
C. A new group of analysts need to be able to place hosts under Network Containment
D. Your organization has resources that need to be accessible when hosts are network contained

Answer: D

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.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 122

How many days will an inactive host remain visible within the Host Management or Trash pages?

A. 45 days
B. 15 days
C. 90 days
D. 120 days

Answer: C

Explanation:

An inactive host will remain visible within the Host Management or Trash pages for 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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 123

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

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.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 124

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: C

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 125

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: B

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 126

When performing targeted filtering for a host on the Host Management Page, which filter bar attribute is NOT case-sensitive?

A. Username
B. Model
C. Domain
D. Hostname

Answer: D

Explanation:

When performing targeted filtering for a host on the Host Management Page, the filter bar attribute that is not case-sensitive is Hostname. The Hostname attribute allows you to filter hosts by their computer name or DNS name. The Hostname filter is not case-sensitive, meaning that it will match hosts regardless of the capitalization of their names. For example, filtering by hostname=DESKTOP- 1234 will match hosts with names such as DESKTOP-1234, desktop-1234, or Desktop-12342.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 127

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: A

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 128

Which report lists counts of sensors in Reduced Functionality Mode (RFM) for all operating system types, and tracks how long a sensor version will be supported?

A. Reduce Functionality Audit Report
B. Sensor Health Report
C. Sensor Coverage Lookup
D. Inactive Sensor Report

Answer: C

Explanation:

The report that lists counts of sensors in Reduced Functionality Mode (RFM) for all operating system types, and tracks how long a sensor version will be supported is Sensor Coverage Lookup. The Sensor Coverage Lookup report allows you to view and compare the sensor versions and coverage status for each operating system type in your environment. You can use this report to identify any sensors that are in RFM or are approaching end-of-life (EOL) support. You can also view the release date and EOL date for each sensor version3.
Reference: 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 129

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

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.

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

Question: 130

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

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.

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

Question: 131

What is likely the reason your Windows host would be in Reduced Functionality Mode (RFM)?

A. Microsoft updates altering the kernel

B. The host lost internet connectivity

C. A misconfiguration in your prevention policy for the host

D. A Sensor Update Policy was misconfigured

Answer: B

Explanation:

The likely reason your Windows host would be in Reduced Functionality Mode (RFM) is that the host lost internet connectivity. RFM is a mode that limits the sensor's functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% 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. Losing internet connectivity is a common cause of RFM, as it prevents the sensor from communicating with the Falcon cloud. A misconfiguration in your prevention policy or sensor update policy will not cause RFM, as these policies are applied by the Falcon cloud and do not affect the sensor's license, network, or certificate status. Microsoft updates altering the kernel may cause compatibility issues with the sensor, but not RFM3.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike 3: How to Become a CrowdStrike Certified Falcon Administrator

Question: 132

On the Host management page which filter could be used to quickly identify all devices categorized as a "Workstation" by the Falcon Platform?

A. Status
B. Platform
C. Hostname
D. Type

Answer: D

Explanation:

The filter that could be used to quickly identify all devices categorized as a "Workstation" by the Falcon Platform on the Host Management page is Type. The Type filter allows you to filter hosts by their device type, such as workstation, server, or domain controller. The device type is assigned to each host based on their Active Directory domain structure. You can use the Type filter to quickly identify all hosts that have the workstation type assigned in their domain2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 133

Where in the console can you find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM)?

A. Host Dashboard
B. Host Management > Filter for RFM
C. Inactive Sensor Report
D. Containment Policy

Answer: B

Explanation:

The place in the console where you can find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM) is Host Management > Filter for RFM. The Host Management page allows you to view and manage all hosts in your environment that have Falcon sensors installed. You can use the filter bar to filter hosts by various attributes, such as status, platform, type, or group. You can also filter hosts by health events, such as RFM, which is a mode that limits the sensor's functionality due to license expiration, network connectivity

loss, or certificate validation failure. By filtering for RFM, you can see a list of all hosts that are in this mode1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 134

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: D

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 135

When editing an existing IOA exclusion, what can NOT be edited?

A. The IOA name
B. All parts of the exclusion can be changed
C. The exclusion name
D. The hosts groups

Answer: A

Explanation:

When editing an existing IOA exclusion, the IOA name cannot be edited. 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. The IOA name is a predefined name that identifies the type of IOA behavior that you want to exclude, such as "Suspicious Process Execution - Script Interpreter Executing File". The IOA name cannot be changed when editing an existing IOA exclusion, as it is linked to a specific IOA rule in the Falcon platform. However, you can edit other parts of the IOA exclusion, such as the exclusion name, the hosts groups, and the filter criteria2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 136

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

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.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 137

Which of the following is NOT an available action for an API Client?

A. Edit an API Client
B. Reset an API Client Secret
C. Retrieve an API Client Secret
D. Delete an API Client

Answer: C

Explanation:

The option that is not an available action for an API Client is Retrieve an API Client Secret. An API Client is an entity that represents a user or application that can access the Falcon platform

programmatically via the Falcon APIs. An API Client has an API Client ID and an API Client Secret, which are used for authenticating and authorizing API requests. You can create and manage API Clients in the API Clients and Keys page in the Falcon console. The available actions for an API Client are Edit an API Client, Reset an API Client Secret, and Delete an API Client. You cannot retrieve an API Client Secret after it has been created, as it is only displayed once during creation for security reasons2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 138

How can a API client secret be viewed after it has been created?

A. Within the API management page, API client secrets can be accessed within the "edit client" functionality
B. The API client secret must be reset or a new client created as the secret cannot be viewed after it has been created
C. The API client secret can be provided by support via direct email request from a Falcon Administrator
D. Selecting "show secret" within the 3-dot dropdown menu will reveal the secret for the selected api client

Answer: B

Explanation:

The way an API client secret can be viewed after it has been created is that the API client secret must be reset or a new client created as the secret cannot be viewed after it has been created. As explained in question 137, an API client secret is only displayed once during creation for security reasons. If you lose or forget your API client secret, you cannot view it again in the Falcon console. You have two options to resolve this issue: either reset your API client secret or create a new API client. Resetting your API client secret will generate a new secret for your existing API client, which will invalidate any previous secret. Creating a new API client will generate a new API client ID and secret, which will require you to update any applications or scripts that use the Falcon APIs2.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 139

What will happen to a host if it is not assigned a Sensor Update policy?

A. The host will uninstall the Sensor and provide an alert to the installation team
B. The host will automatically update to the newest sensor version and auto-update to future release
C. The host will automatically create a custom Sensor Update policy
D. The host will use the Default Sensor Update policy

Answer: D

Explanation:

The option that describes what will happen to a host if it is not assigned a Sensor Update policy is

that the host will use the Default Sensor Update policy. 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. However, if a host is not assigned to a specific Sensor Update policy, it will inherit the settings from the Default Sensor Update policy. The Default Sensor Update policy is a “catch-all” policy that is enabled by default and has the “Uninstall and Maintenance Protection” feature turned on. You can modify the settings of the Default Sensor Update policy, but you cannot delete or disable it1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 140

Which statement describes what is recommended for the Default Sensor Update policy?

A. The Default Sensor Update policy should align to an organization's overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible
B. The Default Sensor Update should be configured to always automatically upgrade to the latest sensor version
C. Since the Default Sensor Update policy is pre-configured with recommend settings out of the box, configuration of the Default Sensor Update policy is not required
D. No configuration is required. Once a Custom Sensor Update policy is created the Default Sensor Update policy is disabled

Answer: A

Explanation:

The statement that describes what is recommended for the Default Sensor Update policy is that the Default Sensor Update policy should align to an organization's overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible. As explained in question 139, the Default Sensor Update policy is a "catch-all" policy that applies to any host that is not assigned to a specific Sensor Update policy. Therefore, it is recommended that the Default Sensor Update policy should align to your organization's overall sensor updating practice, such as how frequently and how quickly you want to update your sensors. It is also recommended that you leverage the Auto N-1 and Auto N-2 configurations, which allow you to automatically update your sensors to the latest or second-latest sensor version without requiring manual intervention1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 141

Why do Sensor Update policies need to be configured for each OS (Windows, Mac, Linux)?

A. To bundle the Sensor and Prevention policies together into a deployment package
B. Sensor Update policies are OS dependent
C. To assist with auditing and change management
D. This is false. One policy can be applied to all Operating Systems

Answer: B

Explanation:

Sensor Update policies need to be configured for each OS (Windows, Mac, Linux) because Sensor Update policies are OS dependent. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. 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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 142

What is the purpose of the Default Sensor Policy?

A. A mechanism to deploy the oldest supported version of the Falcon Sensor.
B. Tests the sensor configuration settings before deployment.
C. Used to reset all sensor settings to Default.
D. Acts as a "catch all" policy if no other Sensor Policies are applied.

Answer: D

Explanation:

The purpose of the Default Sensor Policy is that it acts as a “catch all” policy if no other Sensor Policies are applied. A Sensor Policy is a policy that defines the detection and prevention settings for the Falcon sensor on a host. You can create and assign custom Sensor Policies to different hosts or groups in your environment. However, if a host is not assigned to a specific Sensor Policy, it will inherit the settings from the Default Sensor Policy. The Default Sensor Policy is a “catch-all” policy that is enabled by default and has the “Malware Protection” feature turned on. You can modify the settings of the Default Sensor Policy, but you cannot delete or disable it1.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 143

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

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 144

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

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.
Reference: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

Question: 145

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

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.
Reference: 2: Cybersecurity Resources | CrowdStrike

Question: 146

What is the purpose of the Machine-Learning Prevention Monitoring Report?

A. It is designed to give an administrator a quick overview of machine-learning aggressiveness settings as well as the numbers of items actually quarantined
B. It is the dashboard used by an analyst to view all items quarantined and to release any items deemed non-malicious
C. It is the dashboard used to see machine-learning preventions, and it is used to identify spikes in activity and possible targeted attacks
D. It is designed to show malware that would have been blocked in your environment based on different Machine-Learning Prevention settings

Answer: D

Explanation:

Machine-Learning Prevention Monitoring dashboard: Use this dashboard to view malware that would have been blocked in your environment over the selected timeframe based on different Machine Learning Prevention settings (Cautious, Moderate, Aggressive or Extra Aggressive).

Question: 147

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: A

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.

Reference: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

Question: 148

The Customer ID (CID) is important in which of the following scenarios?

A. When adding a user to the Falcon console under the Users application
B. When performing the sensor installation process
C. When setting up API keys
D. When performing a Host Search

Answer: B

Explanation:

The Customer ID (CID) is important in which of the following scenarios: when performing the sensor installation process and when setting up API keys. The CID is a unique identifier for your organization that is required for authenticating your sensor installation and communication with the Falcon cloud. You need to provide your CID when installing the Falcon sensor on a host, either by using a command-line parameter or by using the falconctl tool. The CID is also required for setting up API keys, which are used for accessing the Falcon platform programmatically via the Falcon APIs. You need to provide your CID when creating an API client and key in the API Clients and Keys page in the Falcon console.

Reference: : [Cybersecurity Resources | CrowdStrike]

Question: 149

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

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.
Reference: : [Cybersecurity Resources | CrowdStrike]

Question: 150

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

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.
Reference: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

Question: 151

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

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.
Reference: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

Question: 152

You have a Windows host on your network in Reduced functionality mode (RFM). While the system is in RFM, which of the following is TRUE?

A. System monitoring will be unavailable
B. Event reporting will be unavailable
C. Prevention patterns will not be triggered
D. Some detection patterns and preventions will not be triggered

Answer: D

Explanation:

The option that is true when a Windows host is in Reduced Functionality Mode (RFM) is that some detection patterns and preventions will not be triggered. RFM is a mode that limits the sensor's functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% 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 cloud. This means that some detection patterns and preventions that rely on telemetry, machine learning, or cloud analysis will not be triggered.
Reference: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

Question: 153

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: B

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.

Reference: : [Cybersecurity Resources | CrowdStrike]