CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: B

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 2

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.

Correct Answer: D

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 3

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

Correct Answer: C

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 4

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

Correct Answer: C

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

QUESTION 5

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

Correct Answer: B

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 6

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

Correct Answer: D

The option that describes how sensor update precedence is determined when a host belongs to more than one host group is that all of the host\\'s groups are examined in aggregate and the policy with highest precedence is applied to the host. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. You can create and assign custom Sensor Update policies to different hosts or groups in your environment. Each Sensor Update policy has a precedence value, which determines its priority over other policies. The higher the precedence value, the higher the priority. If a host belongs to more than one host group, each with a different Sensor Update policy assigned, then all of the host\\'s groups are examined in aggregate and the policy with highest precedence among them is applied to the host. References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

QUESTION 7

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

Correct Answer: A

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 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

Correct Answer: D

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

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

Correct Answer: D

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.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 10

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

Correct Answer: C

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.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 11

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

Correct Answer: B

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 12

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

Correct Answer: D

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 13

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

Correct Answer: A

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 14

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

Correct Answer: A

" 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 15

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

Correct Answer: B

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.