CrowdStrike Falcon Administrator Exam

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(s): B

---

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(s): B

---

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(s): D

---

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(s): C

---

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(s): A

---

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(s): B

---

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(s): C

---

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(s): D

---

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(s): B

---

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(s): D

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(s): D

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(s): A

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(s): B

---

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(s): A

---

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(s): A

---

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(s): B

---

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(s): A

---

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

A. 1

B. 2

C. 0

D. 3

Answer(s): D

---

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(s): D

---

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(s): A
