



- Expert Verified, Online, **Free**.

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

Community vote distribution

B (89%)

11%

🗳️ 👤 **plantvast** Highly Voted 2 years, 3 months ago

Selected Answer: B

In glob, single asterisk is used 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.

upvoted 6 times

🗳️ 👤 **vsnt89** Most Recent 8 months ago

Selected Answer: A

B is correct.

upvoted 1 times

🗳️ 👤 **lightmagenta** 1 year, 4 months ago

b is the answer

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

🗳️ 👤 **FerbOP** 2 years ago

B is correct

upvoted 2 times

🗳️ 👤 **MSKid** 2 years ago

Correct for b

upvoted 1 times

🗳️ 👤 **Reddington0214** 2 years, 2 months ago

B is correct

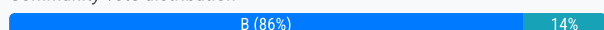
upvoted 1 times

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"

Correct Answer: B

Community vote distribution



🗳️ 👤 **AntiVirusAshok** 7 months ago

Selected Answer: B

Option D, "Using IOC Management, add the hash of the binary in question and set the action to 'No Action,'" would not be effective because it doesn't actively prevent the false positives. By setting the action to "No Action," the system would continue to detect the binary but simply not take any action on it. This means the false positives would still appear in your detection logs, potentially cluttering them and making it harder to identify genuine threats.

On the other hand, setting the action to "Allow" (Option B) ensures that the binary is recognized as safe and prevents it from being flagged in the future, thus keeping your detection logs clean and focused on actual threats.

upvoted 1 times

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: B

Option B is the correct because it won't generate detection while option D will keep generating detection but won't take any action.

upvoted 1 times

🗳️ 👤 **SuperDuperReverb** 1 year, 2 months ago

@DarkieCopy Allow is present in IOC, I just looked. Allow means it will not log the detection, "No Action" means it will still collect data on occurrences.

upvoted 1 times

🗳️ 👤 **DarkieCopy** 1 year, 5 months ago

Selected Answer: D

Got to disagree with everyone: I think D is correct answer.

IOC management only allows "Detect only" and "No Action" among the possible actions, checked in console. Same happens in question #12. "Detect only" and "No Action" are the only possibilities in IOC management

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 3 months ago

Check for Hash, for IP and Domain you have only Detect only and No Action

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

🗳️ 👤 **FerbOP** 2 years ago

B - Allow, do not detect

upvoted 1 times

🗳️ 👤 **Reddington0214** 2 years, 2 months ago

Selected Answer: B

I think B is correct

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (95%)

5%

vsnt89 8 months ago

Selected Answer: D

The correct answer is D. Here is the explanation taken from the official CrowdStrike documentation:

"On the Containment Policy page, you can allow IP addresses over which your hosts will always be allowed to communicate, even if a host is contained."

upvoted 1 times

AntiVirusAshok 9 months, 1 week ago

Selected Answer: C

Option C is correct:

While defining allowed IP addresses over which your hosts will communicate when contained is important, it is typically part of a broader network configuration or security policy rather than the primary purpose of a containment policy.

A containment policy specifically focuses on the conditions or triggers that necessitate placing a machine into network containment, such as detecting a critical threat. This helps ensure that immediate action is taken to isolate the affected machine and prevent the spread of potential threats.

upvoted 1 times

AntiVirusAshok 9 months, 1 week ago

Option C is correct:

While defining allowed IP addresses over which your hosts will communicate when contained is important, it is typically part of a broader network configuration or security policy rather than the primary purpose of a containment policy.

A containment policy specifically focuses on the conditions or triggers that necessitate placing a machine into network containment, such as detecting a critical threat. This helps ensure that immediate action is taken to isolate the affected machine and prevent the spread of potential threats.

upvoted 1 times

CyberMacadamia 1 year, 1 month ago

Selected Answer: D

D is correct, can be seen in UI under Host Setup and Management > Containment Policy > Add allowlist entry

upvoted 3 times

AntiVirusAshok 9 months, 1 week ago

While defining allowed IP addresses over which your hosts will communicate when contained is important, it is typically part of a broader network configuration or security policy rather than the primary purpose of a containment policy.

A containment policy specifically focuses on the conditions or triggers that necessitate placing a machine into network containment, such as detecting a critical threat. This helps ensure that immediate action is taken to isolate the affected machine and prevent the spread of potential threats.

upvoted 1 times

diegofretec 1 year, 7 months ago

El D es el correcto

upvoted 2 times

🗨️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 3 times

🗨️ 👤 **MSKid** 1 year, 12 months ago

Selected Answer: D

Yup, its D

upvoted 3 times

🗨️ 👤 **FerbOP** 2 years ago

Selected Answer: D

D, Network traffic allowlist

upvoted 3 times

🗨️ 👤 **chaos_mob** 2 years ago

Selected Answer: D

Checked the portal and it is D

upvoted 3 times

🗨️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: D

D is correct, 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.

upvoted 3 times

🗨️ 👤 **ShuliAbba** 2 years, 3 months ago

Verified with Falcon's documentation - D is correct.

upvoted 3 times

🗨️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: D

Tested on Falcon. Containment policy is only used to allow communication to specific IPs or IP ranges when a host is contained.

upvoted 2 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **AntiVirusAshok** 9 months, 1 week ago

Selected Answer: C

This means that an administrator can apply an exclusion rule to as many groups of hosts as needed without any restrictions.

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 3 months ago

Selected Answer: C

no limit

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

There is no limit tested in the ui

upvoted 2 times

🗳️ 👤 **LGlif** 1 year, 12 months ago

Selected Answer: C

the answer is C

upvoted 3 times

🗳️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: C

I agree, C is the right answer, I checked in console that when I tried to select some host groups, in the moment I tried to select a 4th group it does not become selected not allowing to add more than 3 groups.

upvoted 2 times

🗳️ 👤 **JSN7117** 1 year, 10 months ago

YOu say ou agree but your last sentence contradicts your statement.

upvoted 2 times

🗳️ 👤 **Roy_So** 2 years, 2 months ago

Selected Answer: C

Tested. C is the correct answer.

upvoted 2 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: C

Tested on Falcon console. Any amount of host groups or all hosts can be added to an exclusion.

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: A

A is the correct one.

upvoted 1 times

🗳️ 👤 **AntiVirusAshok** 9 months, 1 week ago

Selected Answer: A

To use the "Connect to Host" feature and gather additional information directly from the host, you need the Real Time Responder role added to your user account

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: A

A is correct, You need RTR not just FA.

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: A

You must have RTR role to connect to a host. The Falcon Administrator role does not include access to real time response.

upvoted 2 times

🗳️ 👤 **chaos_mob** 2 years ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **andreiushu** 2 years, 2 months ago

Selected Answer: A

A is correct answer

upvoted 1 times

🗳️ 👤 **Roy_So** 2 years, 2 months ago

Selected Answer: A

A is the correct answer x 2

upvoted 1 times

🗳️ 👤 **AlexPuga** 2 years, 2 months ago

Selected Answer: A

A is correct answer

upvoted 1 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

The correct answer is A - Real-Time responder.

upvoted 1 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: A

Only the Real Time Responder roles can allow you to use the Connect to Host option (RTR) in Host Management.

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **fosfor** 3 months, 3 weeks ago

Selected Answer: B

B is correct, tested in UI
upvoted 1 times

🗲️ 👤 **vsnt89** 8 months ago

Selected Answer: B

B is the correct.
upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct, tested in UI
upvoted 2 times

🗲️ 👤 **FerbOP** 2 years ago

Selected Answer: B

B is correct
upvoted 1 times

🗲️ 👤 **Reddington0214** 2 years, 2 months ago

Selected Answer: B

B is the Correct Answer
upvoted 1 times

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"

Correct Answer: C

Community vote distribution

C (100%)

vsnt89 8 months ago

Selected Answer: C

C is correct.

upvoted 1 times

sbag0024 1 year, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

FerbOP 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

Reddington0214 2 years, 2 months ago

Selected Answer: C

C is a possible answer, however when you created a new RTR Rules, the default setting is disabled and you will just add the host group

For D that is also possible> However, the option is to add host name rather than host group.

upvoted 2 times

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

Community vote distribution

D (100%)

🗲️ 👤 **vsnt89** 8 months ago

Selected Answer: D

D is the correct one.

upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: D

D is correct , tested in UI

upvoted 1 times

🗲️ 👤 **FerbOP** 2 years ago

Selected Answer: D

D is correct

upvoted 2 times

🗲️ 👤 **Reddington0214** 2 years, 2 months ago

Selected Answer: D

Tested in the Falcon Console

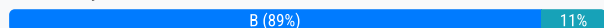
upvoted 1 times

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 fulfil 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

Community vote distribution



🗳️ **anathi** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

🗳️ **vsnt89** 8 months ago

Selected Answer: B

I believe it's the option B.

Knowing that only RTR roles allow you to get remote access to a workstation, I assume these are the potential option. Then I read on the documentation that RTR- Responder allows you to extract file and this is not being asked on the question, so I strongly believe that B is the correct option.

upvoted 1 times

🗳️ **crowdstrikerz** 1 year, 5 months ago

Selected Answer: C

checked

upvoted 1 times

🗳️ **Manuneethi** 1 year, 9 months ago

Also Falcon Analyst-Ready Only having more options then Real Time Responder-Read Only Analyst according to CrowdStrike Original Console note. You can Falcon Analyst-Read only as one more role. that's it.

upvoted 1 times

🗳️ **Manuneethi** 1 year, 9 months ago

C Only correct. The question itself mentioned Falcon Analyst, he needed additional rights to view all logs. So Falcon Analyst- Read Only Correct

upvoted 1 times

🗳️ **Soma7** 1 year, 10 months ago

B is correct answer

upvoted 1 times

🗳️ **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct, checked in the docs

upvoted 1 times

🗳️ **uday1985** 1 year, 11 months ago

B.. confirmed in portal

upvoted 1 times

🗳️ **FerbOP** 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ 👤 **FerbOP** 1 year, 4 months ago

to get into the system and see the files remotely you need RTR role
upvoted 1 times

🗨️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: B

I Agree, the B is the correct answer.

The Falcon Analyst do not have any RTR permission, so it is not able to connect to any host or list files, of course the real time download of files is not allowed.

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 approximated profile for the requested capabilities.

upvoted 1 times

🗨️ 👤 **andreiushu** 2 years, 2 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

🗨️ 👤 **ShuliAbba** 2 years, 3 months ago

I think it would be Real Time Responder - Read Only Analyst. since the RTR admins are probably capable of everything with RTR and RTR Active Responder can extract files from the machine while in the question the ask not to.

upvoted 1 times

🗨️ 👤 **ShuliAbba** 2 years, 3 months ago

@plantvast - but which one?

upvoted 1 times

🗨️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: B

Questions is talking about viewing files and contents on managed hosts which is only possible using Real-Time Response (RTR).

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: D

The answer is the D.

Within the Machine Learning Exclusion, you can configure a path which won't be scanned by the sensor.

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **06a3353** 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **chaos_mob** 2 years ago

Selected Answer: D

D is the only one that makes sense

upvoted 1 times

🗳️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: D

The right answer is D.

Containment Policy, is a allowlist of IPs and CIDR networks allowed in the moment of a host containment.

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.

upvoted 1 times

🗳️ 👤 **AntiVirusAshok** 9 months, 1 week ago

Containment mainly focuses on isolating the machine and triggering detection while the machine is contained

upvoted 1 times

🗳️ 👤 **Reddington0214** 2 years, 2 months ago

Agreed on the voted answer

upvoted 1 times

🗨️ 👤 **ShuliAbba** 2 years, 3 months ago

The correct answer is D!

someone in Examtopics gotta re-check it.

upvoted 2 times

🗨️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: D

Machine Learning exclusions are self-service allowlisting method for when you wish to reduce false positive detections.

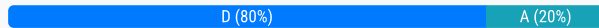
upvoted 1 times

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

Correct Answer: D

Community vote distribution



🗲️ 👤 **Armful** 1 week, 4 days ago

Selected Answer: A

Can only block these IOCs on mobile devices.

upvoted 1 times

🗲️ 👤 **vsnt89** 8 months ago

Selected Answer: D

It's the option D, checked.

upvoted 1 times

🗲️ 👤 **Rahul29** 1 year, 9 months ago

i dont see any option is HostManagement to disable it.

upvoted 1 times

🗲️ 👤 **vsnt89** 8 months ago

Once you are in Host Management, click on any host, then go to the 3 dots in the right end and you will find this option on the menu.

upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: D

D is correct , tested in the UI

upvoted 1 times

🗲️ 👤 **andreiusu** 2 years, 2 months ago

Selected Answer: D

D is the correct answer

upvoted 1 times

🗲️ 👤 **Reddington0214** 2 years, 2 months ago

Selected Answer: D

D is the correct answer, Tested on Falcon Console

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (88%)

12%

🗳️ **999R** 3 months, 2 weeks ago

Selected Answer: A

I think the idea is IOC are indicator of compromise i.e which are artifacts after the attack happened but IOA is something we do for proactive detection, so blocking is done by IOA not IOC. Hence i'll go with A.

upvoted 1 times

🗳️ **vsnt89** 8 months ago

Selected Answer: A

The correct option is A because the IOC Management doesn't offer any action for blocking purposes.

upvoted 1 times

🗳️ **CyberMacadamia** 1 year, 1 month ago

Selected Answer: A

Answer is A (However I initially thought C) - Under Endpoint Security > IOC Management > Add Indicators, you can add Hashes, Domains, and IPs. However!

- IPs: You are unable to block IP addresses and can only detect or no action.

- Domains: You are unable to block IP addresses and can only detect or no action.

upvoted 1 times

🗳️ **diegofretec** 1 year, 6 months ago

Selected Answer: A

Yo creo que la respuesta es A, ya que con IOC no se puede bloquear. Solo detectar o no tomar accion.

upvoted 1 times

🗳️ **DarkieCopy** 1 year, 9 months ago

Answer is A.

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 last one the closest to "block".

So, C is discarded because IOC does not block, and A might be the correct answer, despite not having a "block" option.

upvoted 2 times

🗳️ **Manuneethi** 1 year, 9 months ago

C is Exactly Correct according to CS Falcon and there is 5 options under IOC Management to in the right side corner one button having : Add Hashes, Domain, IP Addresses, Import with Metadata, see Audit Log. Better before sitting for CCFA-200 Exam, verify the options under CS Console or CS Documentation.

upvoted 1 times

🗳️ **sbag0024** 1 year, 10 months ago

Selected Answer: A

A seems correct though the IOA option in the UI is to "kill" the process. There is not a way to block.

upvoted 1 times

🗳️ **FerbOP** 2 years ago

Selected Answer: A

A is correct. Custom IOA rule group can be used to block process associated with IP and domain

upvoted 2 times

🗨️ **JakeUK** 2 years ago

You can add domains to IOC management but the only actions are Detect only or no action therefore the answer is A an IOA rule should be used to block it

upvoted 2 times

🗨️ **Nafil_46** 2 years ago

Selected Answer: A

we can't block IP's in IOC management but we could block domains only for mobile devices. Since question is generic, Answer is A

upvoted 3 times

🗨️ **3xploit** 2 years ago

Selected Answer: C

The Answer is C ! Tested in CS (Hash/Domain /IP)

upvoted 2 times

🗨️ **Belrose** 2 years, 1 month ago

Selected Answer: A

The A is the right answer.

The only available actions for domains and IPs are Detect only and No action, so it is not possible to prevent them. Only hashes can be blocked with the use of IOCs.

upvoted 1 times

🗨️ **im2ca** 2 years, 1 month ago

Option A is the right one, you can add ip, domains and hashes in IOC's but cant take any action other then detect or No action. To block them IOA rule is required where kill process will act as a BLOCK

upvoted 2 times

🗨️ **Jer91** 2 years, 1 month ago

Hello guys, it's C but on cloud EU it's not possible for IP and domain unfortunately. On US cloud yes it's possible.

upvoted 1 times

🗨️ **Prr0** 2 years, 1 month ago

Checked on Falcon, Answer is C

upvoted 1 times

🗨️ **andreiushu** 2 years, 2 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

🗨️ **kgbac** 2 years, 2 months ago

you can't block this IP address on Falcon

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Jcrew929** 9 months, 1 week ago

B is correct - checked with Falcon
upvoted 1 times

🗳️ 👤 **Midhunkollam** 1 year, 9 months ago

B is right
upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B ? going with B as its the only one that has "host" and "admin in it.
upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: B

B is correct
upvoted 1 times

🗳️ 👤 **Reddington0214** 2 years, 2 months ago

B is correct.
upvoted 2 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: B

Prevention Hash Manager is not a real role. The 3 other roles do not exist unless you remove the word "Host". Therefore, the Falcon Administrator is the only role that is able to edit groups and policies.
upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: A

A is the correct answer. I just checked on Falcon console.

upvoted 1 times

🗳️ 👤 **Jcrew929** 9 months, 1 week ago

Answer is A: Tested in Falcon Console

upvoted 1 times

🗳️ 👤 **boombr** 1 year, 4 months ago

Selected Answer: A

TEST on Console CS

upvoted 2 times

🗳️ 👤 **Manuneethi** 1 year, 9 months ago

Only Option Available under CS Falcon Console : First Name and Last Name . no other option to make changes.

upvoted 2 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: A

A is correct. Tested in the UI

upvoted 2 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: A

A is correct.verified from console.

upvoted 2 times

🗳️ 👤 **Reddington0214** 2 years, 2 months ago

I agree to ShuliAbba, Tested on Falcon Console

upvoted 1 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

@plantvast is correct, the site is wrong.

tested on lab - First and Last names can be changed.

upvoted 1 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: A

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.

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **diegofretec** 6 months, 3 weeks ago

Selected Answer: A

A es la correcta

upvoted 1 times

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **MSKid** 11 months, 4 weeks ago

Selected Answer: A

A correct

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **andreiushu** 1 year, 2 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

🗲️ 👤 **ShuliAbba** 1 year, 3 months ago

A looks correct indeed.

B & D - are automated policies.

C - is not automatic at all, the user has to do it 100% manually.

upvoted 3 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: B

B is correct because on the Containment Policy page, you can allow IP addresses over which your hosts will always be allowed to communicate, even if a host is contained.

upvoted 1 times

🗳️ 👤 **diegofretec** 1 year, 6 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Midhunkollam** 1 year, 9 months ago

B is correct

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct, that is the whole point of containment

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Jek88** 2 years, 2 months ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

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

Correct Answer: A

Community vote distribution



diegofretec 6 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Manuneethi 9 months, 2 weeks ago

A is correct : Custom Blocking enables blocklisting by hash, via hashes you add to IOC Management with the option set to Block.

upvoted 1 times

sbag0024 10 months, 2 weeks ago

Selected Answer: C

C? bad question imo.

upvoted 2 times

MSKid 11 months ago

Selected Answer: A

Sounds like A to me:

Falcon allows you to upload hashes from your own black or white lists. To enable 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.

upvoted 1 times

FerbOP 1 year ago

Selected Answer: C

C is correct - Block processes matching hashes that you add to IOC Management with action Block

upvoted 1 times

3xploit 1 year, 1 month ago

Selected Answer: A

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

A for me

upvoted 2 times

im2ca 1 year, 1 month ago

Selected Answer: D

AUTO, N-1, N-2

upvoted 2 times

testmailuc 1 year, 1 month ago

Selected Answer: A

Check here:

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

upvoted 1 times

Jek88 1 year, 2 months ago

C is the correct answer.

upvoted 2 times

🗨️ 👤 **testmailuc** 1 year, 1 month ago

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

upvoted 2 times

🗨️ 👤 **kgbac** 1 year, 2 months ago

Prevention policies don't block custom IOC management you can add link to custom IOA rules. That mean C is the correct answer.

upvoted 2 times

🗨️ 👤 **testmailuc** 1 year, 1 month ago

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

upvoted 2 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

@plantvast - I think you might be wrong because you cannot block IPs and domains, only hashes in the IOC + as written in the policy section "Block processes matching hashes that you add to IOC Management with the action set to "Block" or "Block, hide detection".

upvoted 1 times

🗨️ 👤 **plantvast** 1 year, 3 months ago

You can actually add hashes, domains and IP addresses on IOC management. Navigate to the page in Falcon and attempt to a new indicator and the options will appear.

upvoted 1 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

you are right and wrong my friend, adding IPs and domains in the IOC is indeed possible, but not with "block" action on them - only "detect" or "no action".

upvoted 2 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

from the "Custom Blocking" policy section - "Block processes matching hashes that you add to IOC Management with the action set to "Block" or "Block, hide detection".

upvoted 2 times

🗨️ 👤 **plantvast** 1 year, 3 months ago

Selected Answer: B

Custom blocking in prevention policies refers to hashes, ips, and domains added to IOC Management.

upvoted 1 times

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

- A. 1
- B. 2
- C. 0
- D. 3

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: D

The correct option is D.

upvoted 1 times

🗳️ 👤 **CostumeAbc** 9 months, 3 weeks ago

it's now 4 with "early adopter sensor builds" setting enabled in sensor update policies

* Auto - Early Adopter

* Auto - Latest

* Auto - N-1

* Auto - N-2

upvoted 3 times

🗳️ 👤 **diegofretec** 1 year, 6 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

D is correct. Auto latest, N-1, N-2

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: D

D is correct

upvoted 2 times

🗳️ 👤 **chaos_mob** 2 years ago

Selected Answer: D

correct answer is D

upvoted 1 times

🗳️ 👤 **im2ca** 2 years, 1 month ago

D is the ans

upvoted 1 times

🗳️ 👤 **Roy_So** 2 years, 2 months ago

Selected Answer: D

Should be 3: Auto, N-1, N-2

upvoted 2 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

you are right, the correct answer is D.

upvoted 2 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: D

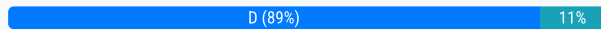
There are 3 options to auto update via sensor update policy for all supported OSes: auto - latest, auto - N-1, auto - N-2
upvoted 2 times

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

Correct Answer: D

Community vote distribution



🗳️ 👤 **diegofrelesc** 8 months, 3 weeks ago

Es el D!

upvoted 1 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct, tested in the UI

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct

upvoted 2 times

🗳️ 👤 **ImpulseEEE** 1 year, 1 month ago

Selected Answer: D

D - 100%

upvoted 2 times

🗳️ 👤 **andreiushu** 1 year, 2 months ago

Selected Answer: D

D is the correct answer. For each prevention policy there is an option to Assign a Host Group

upvoted 3 times

🗳️ 👤 **Reddington0214** 1 year, 2 months ago

Selected Answer: C

C is much a possible answer

upvoted 1 times

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

Community vote distribution

A (83%)

B (17%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: A

Option A

upvoted 1 times

🗳️ 👤 **silva222222** 11 months, 2 weeks ago

Selected Answer: A

<https://www.crowdstrike.com/products/endpoint-security/falcon-insight-edr/faq/>

upvoted 2 times

🗳️ 👤 **Manuneethi** 1 year, 9 months ago

90 days only

upvoted 2 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Shoot it Could be A.Per the CCFA Checklist Notes " 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

upvoted 2 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

Going to go with B, its either B or C . Bad question really.

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

I Think this is C, It says Detection Events. Events are stored for 7 Days

upvoted 1 times

🗳️ 👤 **Synecdoque19** 1 year, 11 months ago

Activity feed (alerts) are kept 90 days. Events (EAM Data) depends on your contract

upvoted 1 times

🗳️ 👤 **SoFi443** 1 year, 11 months ago

I think the right answer should be B

upvoted 2 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: A

A is correct

upvoted 2 times

🗳️ 👤 **options862** 2 years ago

Option - A

Note: CrowdStrike keeps detection data in the cloud for 90 days, after which some of the data gets purged from the database. Null icons indicate that some of the data for a process has started to be nullified. It could be a missing tactic, label, metadata or any part of the information pertaining to that process.

upvoted 2 times

  **plantvast** 2 years, 3 months ago

The wording of the question makes this confusing. Detections themselves are kept for 90 days but event data is only kept for the event retention set.

upvoted 2 times

What information is provided in Logon 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

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

Checking o documentation and found this "Only provides a summary of the last logon activity for users."

upvoted 1 times

🗲️ 👤 **Reddington0214** 1 year, 2 months ago

Selected Answer: B

Upon checking B is the answer

upvoted 2 times

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

Correct Answer: *B*

Community vote distribution

B (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct, checked in the docs

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

B is the correct answer.

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is sorta correct but as Jak88 said
upvoted 1 times

🗨️ **MSKid** 11 months, 2 weeks ago

Selected Answer: B

B is correct
upvoted 1 times

🗨️ **FerbOP** 1 year ago

Selected Answer: B

B - for windows
(FYI...D - for linux)
upvoted 2 times

🗨️ **Jek88** 1 year, 2 months ago

Selected Answer: B

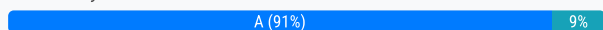
B is the correct answer but with sc.exe query csagent command.
upvoted 2 times

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

Correct Answer: A

Community vote distribution



🗳️ 👤 **diegofretec** 6 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **DarkieCopy** 9 months, 2 weeks ago

Selected Answer: A

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.

Answer is A

upvoted 2 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct, tested in UI

upvoted 1 times

🗳️ 👤 **Shaheen_Falcon** 10 months, 4 weeks ago

A is correct

upvoted 1 times

🗳️ 👤 **JakeUK** 11 months, 3 weeks ago

Selected Answer: A

The correct answer is A - Custom IOA Groups. The prevention policies page separates each policy by Win/Mac/Linux however a specific policy can be assigned to host groups and custom IOA Groups, therefore the answer is A

upvoted 2 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **michalpapi** 1 year ago

Selected Answer: D

If you go to the Prevention policies tab you will see Windows/Mac/Linux policies segregation. Once you choose OS only then you can assign a host group to the specific prevention policy. Each OS has a different set of prevention policies and each prevention policy is assignable to a specific host group. The answer is D.

upvoted 1 times

🗳️ 👤 **chaos_mob** 1 year ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

🗳️ 👤 **kgmangle** 1 year, 1 month ago

Correct Answer is A

upvoted 1 times

🗨️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: A

Answer is A

upvoted 1 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

Correct answer is A :)

upvoted 1 times

🗨️ 👤 **plantvast** 1 year, 3 months ago

Selected Answer: A

The two groups are Host Groups and Custom IOAs

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct, Checked in the docs

upvoted 1 times

🗳️ 👤 **Shaheen_Falcon** 10 months, 4 weeks ago

Answer C

upvoted 1 times

🗳️ 👤 **CXSSP** 11 months ago

Selected Answer: C

definitely C

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: C

Answer C

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

C is the correct answer.

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ **vsnt89** 8 months ago

Selected Answer: C

C is the correct one. Just checked on the documentation.

upvoted 1 times

🗳️ **sbag0024** 1 year, 10 months ago

Selected Answer: C

C is correct, per the docs "Needs more time for install? (ProvNoWait=1),"

upvoted 1 times

🗳️ **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ **im2ca** 2 years, 1 month ago

Selected Answer: C

If your host requires more time to connect, you can override this by using the ProvWaitTime parameter in the command line to increase the timeout to 1 hour.

upvoted 2 times

🗳️ **ShuliAbba** 2 years, 3 months ago

Plantvast is correct, the answer is C.

Here's a quote from the documentation:

"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)."

upvoted 2 times

🗳️ **plantvast** 2 years, 3 months ago

Selected Answer: C

The 2 command that can be used for this scenario are ProvNoWait=1 or ProvWaitTime=(time in milliseconds).

upvoted 2 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: C

C is correct. Just checked.

upvoted 1 times

🗳️ 👤 **kangaru** 1 year, 10 months ago

Change the time range to 30 days will filter inactive hosts MORE than 30 days, not exactly 'last 30 days'

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

C is correct, tested in the UI

upvoted 1 times

🗳️ 👤 **Shaheen_Falcon** 1 year, 10 months ago

C. Under Host setup and management > Managed endpoints > Inactive Sensors. Change the time range to 30 days

upvoted 1 times

🗳️ 👤 **MSKid** 1 year, 11 months ago

Selected Answer: C

C is right

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **chaos_mob** 2 years ago

Selected Answer: C

Checked in the cs portal

upvoted 1 times

🗳️ 👤 **Dave071** 2 years ago

C - %100

upvoted 1 times

🗳️ 👤 **muirice** 2 years, 1 month ago

A and C are both correct tested both of them in my environment.

upvoted 1 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

C is correct, tested in a lab.

upvoted 2 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Jimmy390** 9 months, 3 weeks ago

Selected Answer: B

checked

upvoted 1 times

🗳️ 👤 **hussainuch** 1 year, 4 months ago

Selected Answer: B

upvoted 2 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: B

B is correct, tested in the UI

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: B

B is correct

upvoted 2 times

🗳️ 👤 **kgmangle** 2 years, 1 month ago

Correct Answer is B

upvoted 1 times

🗳️ 👤 **im2ca** 2 years, 1 month ago

Selected Answer: B

tested with CS

upvoted 1 times

🗳️ 👤 **Roy_So** 2 years, 2 months ago

Selected Answer: B

Checked on the Falcon dashboard x 2

upvoted 2 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

B is correct, checked on the Falcon dashboard.

upvoted 2 times

🗳️ 👤 **plantvast** 2 years, 3 months ago

Selected Answer: B

Quarantine & Security Center Registration option must be enabled under Type=Next-Gen Antivirus Category=Quarantine.

upvoted 3 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **diegofretec** 1 year, 6 months ago

Selected Answer: A

You will notice tabs each agent type, Windows, Mac or Linux, will allow specific configuration for the agent updates on each platform.. A IS CORRECT

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: A

A is correct, only one option here..

upvoted 1 times

🗳️ 👤 **MSKid** 1 year, 11 months ago

Selected Answer: A

Right for A

upvoted 1 times

🗳️ 👤 **kgmangle** 2 years, 1 month ago

A is the correct answer

upvoted 1 times

🗳️ 👤 **testmailuc** 2 years, 1 month ago

Selected Answer: A

A is correct.

Verify from here: <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>

upvoted 1 times

🗳️ 👤 **kgbac** 2 years, 2 months ago

A is the correct answer

upvoted 3 times

🗳️ 👤 **testmailuc** 2 years, 1 month ago

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

upvoted 1 times

🗳️ 👤 **ShuliAbba** 2 years, 3 months ago

B sounds more correct...

upvoted 1 times

🗳️ 👤 **testmailuc** 2 years, 1 month ago

You are wrong.

Just check here: <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>

A is correct

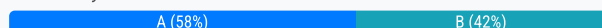
upvoted 1 times

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 click "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 filters if needed) and click Add.

Correct Answer: A

Community vote distribution



🗳️ **fosfor** 3 months, 3 weeks ago

Selected Answer: B

B.

This approach allows for dynamic host management using tags and ensures scalability, as you can add or remove tags to hosts without manually managing static groups.

upvoted 1 times

🗳️ **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

Going with A, tested in UI though you can do this many ways..

upvoted 2 times

🗳️ **xart** 11 months, 3 weeks ago

Selected Answer: A

A is the correct answer since you are assigning a policy to host group.

upvoted 2 times

🗳️ **FerbOP** 1 year ago

I ll go with B. It is saying specific group of hosts. not specific host(Static by hostname)

upvoted 1 times

🗳️ **Dave071** 1 year ago

Since the requirement is a "specific group of hosts", I would go with answer A as static hosts do not change.

upvoted 1 times

🗳️ **kgmangle** 1 year, 1 month ago

Selected Answer: A

Correct Answer is A

1) Policy needs to apply to specific hosts so need to create static Host Group

2) Host Group needs to assign from the desired policy only.

upvoted 2 times

🗳️ **Belrose** 1 year, 1 month ago

Selected Answer: B

I think B is the correct answer.

I see that in A answer tells that "click" Add groups to policy, when it is not possible to click this option, you only can click in the button.

Both host static assignment and tagging are possible ways to select a group of machines, so I think that the right answer is B.

upvoted 3 times

🗳️ **im2ca** 1 year, 1 month ago

Selected Answer: B

B is Correct answer, tested with the CS. IT can be dynamic or static; however, when tags are used it can be any different hosts into a host group and policy applied

upvoted 1 times

🗨️ 👤 **plantvast** 1 year, 3 months ago

Looking back on this now B makes more sense because either dynamic or static groups can be a specific group.

upvoted 2 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

correct, I would definitely go with B.

upvoted 1 times

🗨️ 👤 **ShuliAbba** 1 year, 3 months ago

Why? it could be a specific dynamic group, out of X groups the user has on his dashboard.

it could be also a dynamic group based on Tags...

upvoted 1 times

🗨️ 👤 **plantvast** 1 year, 3 months ago

Selected Answer: A

Questions mentions a specific group of hosts so the answer should be a static group.

upvoted 1 times

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

Community vote distribution

D (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct, tested in UI
upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct
upvoted 1 times

🗲️ 👤 **ShuliAbba** 1 year, 3 months ago

D is correct. tested on lab.
upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗨️ **DarkieCopy** 9 months, 2 weeks ago

Selected Answer: A

A is correct.

Syntax in \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill is incorrect (tested on UI)

upvoted 1 times

🗨️ **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct,

upvoted 1 times

🗨️ **Dave071** 1 year, 1 month ago

A is the correct answer. You can check the regular expression on a regex builder.

upvoted 1 times

🗨️ **Roy_So** 1 year, 2 months ago

Selected Answer: A

A is correct. checked on lab.

upvoted 2 times

🗨️ **sonian** 1 year, 3 months ago

The answer is A. You are using RegEx here and need leading "." to capture www and then need a "." at the end to identify any sites falling under badguydomain.com

upvoted 2 times

🗨️ **plantvast** 1 year, 3 months ago

The syntax for C is correct and this would catch any process trying to reach out to the domain.

upvoted 1 times

🗨️ **ShuliAbba** 1 year, 3 months ago

but where would you put this string - command, parent name, image file name??

I copied the sting in option B to the command line and it suggested a few minor suggestions of "\" or "*"...

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **vsnt89** 8 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **diegofretec** 1 year, 6 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

C is correct. Anything around containing is always going to be in the containment policy.

upvoted 1 times

🗲️ 👤 **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **Dave071** 2 years, 1 month ago

C is correct

upvoted 1 times

🗲️ 👤 **Jek88** 2 years, 2 months ago

C is the correct answer.

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (75%)

A (25%)

🗳️ 👤 **GreenHok** 9 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Gapsiux** 1 year, 3 months ago

B is correct. From CS KB: Stop all behavioural detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

upvoted 2 times

🗳️ 👤 **Manuneethi** 1 year, 9 months ago

B is correct. The option under Exclusion-2nd option IOA Exclusions

upvoted 1 times

🗳️ 👤 **Alex_41** 1 year, 11 months ago

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>

upvoted 2 times

🗳️ 👤 **MSKid** 1 year, 11 months ago

Selected Answer: B

IOA is correct

upvoted 1 times

🗳️ 👤 **xart** 1 year, 11 months ago

Selected Answer: B

IOA Exclusion is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **kgmangle** 2 years, 1 month ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

🗳️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: A

I think the A option is the correct answer.

In IOA actions you can not avoid the detection, you only can monitor, detect or mitigate in any way (Kill process, Block Execution) so it is not possible to hide the detection.

In relation with the IOAs are applied to all the detections in general not only for behavioural detection, so the Machine Learning is the only choice that is related with only behavioural detections, and finally with machine learning detections it is possible avoid the detection and prevention, so I think the most logical answer is A.

upvoted 2 times

🗨️ **im2ca** 2 years, 1 month ago

Selected Answer: B

IOA: Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

upvoted 1 times

🗨️ **Killer44010** 2 years, 1 month ago

Selected Answer: B

CrowdStrike's Machine Learning and behavior based detections known as Indicators of Attack (IOAs)

upvoted 1 times

🗨️ **Killer44010** 2 years, 1 month ago

its B, CrowdStrike's Machine Learning and behavior based detections known as Indicators of Attack (IOAs)

upvoted 1 times

🗨️ **testmailuc** 2 years, 1 month ago

Selected Answer: B

About exclusions we have:

IOA: Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

Machine learnings: For trusted file paths, stop all ML-based detections and preventions, or stop files from being uploaded to the CrowdStrike cloud.
From documentation.

So correct answer is B

upvoted 2 times

🗨️ **Reddington0214** 2 years, 2 months ago

Selected Answer: A

When we say behavioral detection machine learning is much closer

upvoted 1 times

🗨️ **testmailuc** 2 years, 1 month ago

You are wrong. About exclusions we have:

IOA: Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

Machine learnings: For trusted file paths, stop all ML-based detections and preventions, or stop files from being uploaded to the CrowdStrike cloud.

From documentation.

So correct answer is B

upvoted 2 times

🗨️ **kgbac** 2 years, 2 months ago

IOA exclusion ?? B

upvoted 3 times

🗨️ **testmailuc** 2 years, 1 month ago

You are right. Just for documentation confirmation.

About exclusions we have:

IOA: Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

Machine learnings: For trusted file paths, stop all ML-based detections and preventions, or stop files from being uploaded to the CrowdStrike cloud.

From documentation.

So correct answer is B

upvoted 2 times

🗨️ **ShuliAbba** 2 years, 3 months ago

A is correct

upvoted 2 times

  **testmailuc** 2 years, 1 month ago

You are wrong. About exclusions we have:

IOA: Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

Machine learnings: For trusted file paths, stop all ML-based detections and preventions, or stop files from being uploaded to the CrowdStrike cloud.

From documentation.

So correct answer is B

upvoted 2 times

What are custom alerts based on?

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **vsnt89** 8 months ago

Selected Answer: C

C is correct, just checked.

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

C is correct, checked in the UI

upvoted 1 times

🗳️ 👤 **CharlesB2** 1 year, 12 months ago

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.

upvoted 1 times

🗳️ 👤 **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 2 times

🗳️ 👤 **FerbOP** 2 years ago

Correction -Correct answer is B. Custom alerts based on Custom event based triggers.

upvoted 1 times

🗳️ 👤 **Belrose** 2 years, 1 month ago

Selected Answer: C

Accessing to custom alerts you will see a list of predefined alert templates configurables in certain aspects but it is not possible to add new event triggers for new alerts, so I think the C answer is the correct.

upvoted 2 times

🗳️ 👤 **Percy73729** 2 years, 2 months ago

Correct answer is C

upvoted 3 times

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

Correct Answer: B

Community vote distribution

B (100%)

vsnt89 8 months ago

Selected Answer: B

B is correct. This is a common operation in the creation of any API.

upvoted 1 times

sbag0024 1 year, 10 months ago

Selected Answer: B

B is correct, was in the training and in the study docs

upvoted 1 times

CharlesB2 1 year, 12 months ago

Secret is only visbile when creating the API

upvoted 1 times

FerbOP 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

ShuliAbba 2 years, 3 months ago

B is correct.

upvoted 3 times

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 offline 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

Correct Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **vsnt89** 8 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

c is correct

upvoted 1 times

🗲️ 👤 **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **Jek88** 2 years, 2 months ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **hussainuch** 4 months, 3 weeks ago

Selected Answer: D

upvoted 1 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct, though if you drill in C is also correct, question did not ask if you drill into the report.

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Correction - C is correct answer

upvoted 2 times

🗳️ 👤 **FerbOP** 1 year ago

User Name:

*

Account Type:

All

Admin Privileges:

All

Logon Type:

All

Time Range:

7 days

Company:

All

Submit/Hide Filters

User Logon Activities

Company User User Name Account Type Local Admin Privileges Logon Type Logged On Host Logon Time Password Last Set Months since Password Last Set

you can get these details

upvoted 1 times

🗳️ 👤 **kangaru** 1 year ago

Selected Answer: D

If you view the Logon Activities, it only shows you the user last logon activity. If you click into the entry, it redirects you to 'user search' that contains a list detail of logon activities of the user. However, user search is no longer same as 'Logon Activities' here.

upvoted 1 times

🗨️ 👤 **Dave071** 1 year, 1 month ago

I would go with D as you can only view logon activities up to the Last 60 days, and not ALL as C suggests.

upvoted 1 times

🗨️ 👤 **Jer91** 1 year, 1 month ago

It's D, it only give the last logon, not all.

upvoted 1 times

🗨️ 👤 **bbqsauceomg** 1 year, 1 month ago

Selected Answer: D

based on the Training material and the Pre-exam Report Matching game

the answer is D

upvoted 1 times

🗨️ 👤 **andreiushu** 1 year, 2 months ago

Selected Answer: D

I think D is the correct answer

upvoted 1 times

🗨️ 👤 **Jek88** 1 year, 2 months ago

You might be right, as the report gives Logon Type, Logged On Host, and Logon Time for the logon activities. Not still sure between C & D.

upvoted 1 times

🗨️ 👤 **Jek88** 1 year, 2 months ago

C is the correct answer.

upvoted 2 times

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

Community vote distribution

A (100%)

🗳️ 👤 **HereToLearn** 10 months, 2 weeks ago

Selected Answer: A

Bad question but they will change in the test to say "what is the minimum role required to create scripts"
upvoted 1 times

🗳️ 👤 **Shri_24** 12 months ago

A Or D Which is correct
upvoted 1 times

🗳️ 👤 **diegofretec** 1 year ago

Selected Answer: A

Real time reponder script developer no existe
upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: A

A is correct, checked in the docs
upvoted 1 times

🗳️ 👤 **uday1985** 1 year, 5 months ago

. Real Time Responder – Script Developer Does not even exist in the portal
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: A

A is correct
upvoted 1 times

🗳️ 👤 **3xploit** 1 year, 6 months ago

Selected 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.
upvoted 2 times

🗳️ 👤 **Dave071** 1 year, 7 months ago

Answer is A as answer C cannot create scripts.
upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 9 months ago

Selected Answer: A

Correct is A
upvoted 2 times

🗳️ 👤 **ShuliAbba** 1 year, 9 months ago

wrong!!! no such role as "script developer".
the correct answer should be "Real Time Responder - Administrator" that "creates and deploy custom scripts". while the "Active Responder" can also "run certain custom scripts"

upvoted 1 times

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)

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **CyberMacadamia** 7 months, 1 week ago

Selected Answer: B

Trigger > Condition > Action - Found in UI within Falcon Fusion
upvoted 1 times

🗳️ 👤 **diegofretec** 1 year ago

Selected Answer: B

BB is the correct answer
upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: B

B is the correct answer tested in the UI
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: B

B is correct
upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 8 months ago

Selected Answer: B

B is the correct answer.
upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Roy_So** Highly Voted 👍 1 year, 2 months ago

Selected Answer: D

Wrong!! the secret can never be restored once created. > Answer should be D
upvoted 6 times

🗳️ 👤 **jcm3** Most Recent ⌚ 3 months, 4 weeks ago

Selected Answer: D

asdasdasdasd
upvoted 1 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is the only answer. This was in the training and in the study doc
upvoted 1 times

🗳️ 👤 **xart** 11 months, 3 weeks ago

Selected Answer: D

D is the correct answer, although the secret can be reset
upvoted 2 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is corrcet
upvoted 2 times

🗳️ 👤 **im2ca** 1 year, 1 month ago

Selected Answer: D

The API client secret cannot be retrieved after it has been created
upvoted 2 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

Wrong!! the secret can never be restored once created.
upvoted 3 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

hence B is the right answer.
upvoted 2 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

typo? Answer is D
upvoted 2 times

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)

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is the only answer here. It is in the docs
upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is Correct
upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: B

B is the correct answer.
upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct, tested in the UI
upvoted 1 times

🗳️ 👤 **uday1985** 11 months, 3 weeks ago

its A 100% check the platform
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct
upvoted 1 times

🗳️ 👤 **chaos_mob** 1 year ago

Selected Answer: A

verified A
upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: A

In the Falcon console. Only CID is unique
upvoted 3 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

B is TOTALLY WRONG!!!
all Falcon sensors can be downloaded from the host and setup resources > sensor downloads.
upvoted 2 times

🗳️ 👤 **plantvast** 1 year, 3 months ago

Selected Answer: A

Sensor Downloads page in Falcon console
upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: D

D. CS needs to verify the kernel and release the new sensor version, if the kernel isn't certified, then run as RFM.

upvoted 3 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

C is wrong!

The correct answer is D - windows updates. verified with the documentation.

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (86%)

14%

🗳️ 👤 **CyberMacadamia** 7 months, 1 week ago

Selected Answer: D

D. Confirmed within UI - Host Setup and Management > Host Groups
upvoted 1 times

🗳️ 👤 **Technan456** 1 year, 2 months ago

Selected Answer: D

D. Confirmed via UI
upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: D

D is correct tested in the UI
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: D

D is correct
upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 7 months ago

Selected Answer: D

I agree with the D option.
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 assign a group of host to the policy not creating a group of hosts.
upvoted 1 times

🗳️ 👤 **roddiasmacedo** 1 year, 7 months ago

Selected Answer: D

You can groups on host and setup management > host Groups> Create a group;
Letter B is only to create policies and apply groups selected before
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

D
Its the host groups where you create the sensor or host groups not under sensor update policies.
upvoted 1 times



🗳️ 👤 **Jek88** 1 year, 8 months ago

Selected Answer: B

B is the correct answer, not sure what they meant by sensor groups tho.
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 7 months ago

Why is that? How you can create groups from Sensor Update Policies?
upvoted 2 times

  **VJJjo** 1 year, 9 months ago

CORRECT

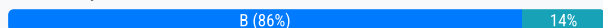
upvoted 1 times

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

Correct Answer: B

Community vote distribution



🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

Going with B , tested in UI
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct
upvoted 1 times

🗳️ 👤 **Dave071** 1 year ago

I would go with B as the requirement is to allow specific internal IP addresses and not the entire internal IP CIDR block.
upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: B

The B is the correct answer, when a host is contained the firewall policy is not working.
If you add a standar firewall rule, how can the product to know wich rules apply in containment status? The answer is defining the firewall containment firewall rules in a diferente place, in this case is defined in the containment pollicy.
upvoted 1 times

🗳️ 👤 **Dr_Falcon** 1 year, 1 month ago

B >> Correct Answer - Tested in LAB
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: C

C should be the correct anqser. Documentation checked. Should be a IP/CIDR range
upvoted 1 times

🗳️ 👤 **kangaru** 1 year ago

It is filtered using CIDR range. But you can create multiple filters to flexibly control more allowed IPs.
upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: B

Correct Ans is B
upvoted 3 times



🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

D is wrong.
C is the correct answer - while a host is contained, you must use the containment policy to allow the host to connect to other IP addresses. verified with the Falcon documentation.
upvoted 1 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

correction - B should be the right answer.

upvoted 1 times

  **testmailuc** 1 year, 1 month ago

C should be the correct anqser. Documentation checked. Should be a IP/CIDR range

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct, only option here

upvoted 1 times

🗳️ 👤 **uday1985** 11 months, 3 weeks ago

C is correct... I tried it and it wont allow you

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: C

Tested in console if you try to elevate the prevention level to a higher than the detection level is not allowed. It is logical because if you detect less things than you are protecting is not congruent.

upvoted 1 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

C is the correct answer - tested on Falcon dashboard.

upvoted 3 times

🗳️ 👤 **plantvast** 1 year, 3 months ago

Selected Answer: C

Tested on Falcon console

upvoted 3 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **CyberMacadamia** 7 months, 1 week ago

Selected Answer: C

Answer should be C

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: C

C is correct, this is right out of the doc

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: C

C is correct answer

upvoted 2 times

🗳️ 👤 **kangaru** 1 year, 6 months ago

Selected Answer: C

D has nothing to do this API

upvoted 1 times

🗳️ 👤 **Dr_Falcon** 1 year, 7 months ago

C. DetectionSummaryEvent stops sending to the Streaming API for that host

Checked at documentation

upvoted 2 times

🗳️ 👤 **Percy73729** 1 year, 8 months ago

Confirmed with documentation. Correct answer is C

upvoted 4 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct,
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct
upvoted 2 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: D

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 differentiated 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.

Definitely the D is the right answer.

upvoted 4 times

🗳️ 👤 **Dr_Falcon** 1 year, 1 month ago

Correct Answer is D - Changes after installation require a registry edit and a host reboot; otherwise, the changes take effect when the sensor is next upgraded. (From documentation)

upvoted 1 times

🗳️ 👤 **ShuliAbba** 1 year, 3 months ago

Tricky question - both B and D could be the right answers.

upvoted 1 times

🗳️ 👤 **marcegg1** 1 year, 2 months ago

Sensor tags are only configured at installation, the falcon groupoing tags are configured in the console. after the installation you can configure the sensor but you'll need to reboot the host

upvoted 2 times

Custom IOA rules are defined using which syntax?

- A. Glob
- B. PowerShell
- C. Yara
- D. Regex

Correct Answer: D

Community vote distribution

D (75%)

13%

13%

🗳️ **CyberMacadamia** 7 months, 1 week ago

Selected Answer: D

D - Regex checked in. UI under Endpoint Security > Configure > Custom IOA Rule Groups. Use REGEX
upvoted 1 times

🗳️ **sbag0024** 1 year, 4 months ago

Selected Answer: D

D Regex. ML is Glob. IOA is Regex
upvoted 1 times

🗳️ **uday1985** 1 year, 5 months ago

Selected Answer: D

When creating an IOA its providing you with this link:

Custom Intelligence via Indicator of Attack

Regex guidelines

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

upvoted 1 times

🗳️ **Pan1c** 1 year, 5 months ago

I believe ML uses Glob, but IOA uses Regex. D.

upvoted 1 times

🗳️ **FerbOP** 1 year, 6 months ago

Selected Answer: D

D - regex

upvoted 1 times

🗳️ **Belrose** 1 year, 7 months ago

Selected Answer: D

From Documentation - Detection and Prevention Policies "The four different rule types provide unique detection parameters that can be configured using supported regex syntax in their fields."

upvoted 2 times

🗳️ **Belrose** 1 year, 7 months ago

From Documentation --> Detection and Prevention Policies

"The four different rule types provide unique detection parameters that can be configured using supported regex syntax in their fields."

Right answer: D - Regex.

upvoted 1 times

🗳️ **im2ca** 1 year, 7 months ago

Selected Answer: B

Regex syntax is used



upvoted 1 times

🗳️ **Lasitha20** 1 year, 7 months ago

Selected Answer: A

Glob is the correct one. Answer is A

upvoted 1 times

  **ShuliAbba** 1 year, 9 months ago

B is wrong!

the correct answer is D - Regex. verified on Falcon console.

upvoted 3 times

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

Community vote distribution

B (78%)

D (22%)

🗳️ 👤 **Brian9296** 5 months ago

Selected Answer: B

Vote for B

upvoted 1 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B and D are correct but B was done in the class

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **kangaru** 1 year ago

Selected 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.

upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: B

In the console all the custom alerts have a Monitoring Frequency, and none can be set as real time, so the D option is not possible and the only feasible option is B.

upvoted 1 times

🗳️ 👤 **im2ca** 1 year, 1 month ago

Selected Answer: D

two reasons: security staff need to see what's going on in their environment in real-time

upvoted 1 times

🗳️ 👤 **Killer44010** 1 year, 1 month ago

Selected Answer: D

Simply getting a report on password logon attempts or file and application usage is not enough, for two reasons: security staff need to see what's going on in their environment in real-time

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

Cannot change the interval. I think the correct answer is B. Interval is prefixed

upvoted 1 times

🗳️ 👤 **ImpulseEEE** 1 year, 1 month ago

Selected Answer: B

B is correct (question is also mentioned in the test exam on CS University)

upvoted 1 times

🗨️ 👤 **basicn00b** 1 year, 2 months ago

The correct answer is B

upvoted 2 times

🗨️ 👤 **Percy73729** 1 year, 2 months ago

Correct answer is A, confirmed on documentation

upvoted 2 times

🗨️ 👤 **testmailuc** 1 year, 1 month ago

Cannot change the interval. I think the correct answer is B. Interval is prefixed

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **nickla1974** 5 months ago

C is correct.

upvoted 1 times

🗳️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: C

It asks how do you assign, as if it is already created. D is not correct. C is the only other option

upvoted 1 times

🗳️ 👤 **Shaheen_Falcon** 1 year, 4 months ago

C is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 7 months ago

Selected Answer: C

To one or more groups you have to create the group first. So C is the correct answer

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 8 months ago

D is the correct answer

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 8 months ago

Sorry did not see to one or more hosts, C should be the correct answer.

upvoted 1 times

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"

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

C is the correct answer.

upvoted 1 times

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*\

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is the only one that could work even though they are all wrong in ways.

upvoted 1 times

🗳️ 👤 **Joe_Kwok** 11 months, 2 weeks ago

No one be a answer.

Answer should be *\Program Files\My Program**

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

Should be A. I am not sure about the \ at the beginning, but the are options not seems correct to me. So excluding everything remains A.

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: A

I believe A is the correct answer, even though the file is mentioned.

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Jraph** 10 months ago

Action can't be blank.
on the empty so A is incorrect.
upvoted 1 times

🗨️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A. found in the doc
upvoted 1 times

🗨️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct
upvoted 1 times

🗨️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

Documentation checked. A is the correct answer
upvoted 1 times

🗨️ 👤 **Reddington0214** 1 year, 2 months ago

Selected Answer: A

A is correct
upvoted 2 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is the only answer here. not a good question

upvoted 1 times

🗨️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B, checked in UI/Docs

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

After checking the documentation should be B

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Maybe D:

Policy precedence determines which policy's configuration settings are applied to a host when the host is a member of more than one policy. You define policies with different precedences to resolve conflicts. Then, when faced with a conflict, the cloud will automatically apply the policy with the higher precedence (1 being higher than 2, which is higher than 3, and so on).

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

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)

Correct Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **Rdxbr** 1 year, 2 months ago

Selected Answer: A

A, is the correct answer.

upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: A

A is the correct answer.

upvoted 1 times

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

Community vote distribution

C (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C, checked in UI
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: C

C is correct. Verified through console
upvoted 1 times

🗳️ 👤 **Rdxbr** 1 year, 2 months ago

Selected Answer: C

Yes, answer C is the true.
upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: C

C is the correct answer.
upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: C

C is correct.

upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: C

C is the correct answer, meaning support portal.

upvoted 1 times

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)

Correct Answer: B

Community vote distribution

B (80%)

D (20%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B, it is AID

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Dave071** 1 year, 1 month ago

Host ID & Agent ID are interchangeable according to documentation.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

B is correct. Its the Agent ID linked with Host Unique Identifies not the CID - Customer ID is for the Site.

upvoted 2 times

🗳️ 👤 **ImpulseEEE** 1 year, 1 month ago

A unique host identifier in Falcon is called Host ID , the closest here could be Agent ID ; so B is Correct !?

upvoted 3 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

B is the correct anwser. Verified through console and documentation

upvoted 2 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: D

D should be the correct answer but it is called Customer ID. Thought could be Agent ID, but that is related to active tokens in installers.

upvoted 1 times

🗳️ 👤 **Reddington0214** 1 year, 2 months ago

Customer ID is the one you used when installing the sensor, Agent ID is the one automatically generated by the system as identifier of the sensor installed in the host so B is Correct

upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A . Found in TS doc

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

All the other choices are wrong. A is the only one makes sense.

upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: A

A is the correct answer.

upvoted 1 times

You need to export a list of all detections 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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct, tested in UI

upvoted 1 times

🗳️ 👤 **LaCubanita** 12 months ago

Selected Answer: C

Correct answer is C, option to export is at the end of the Detection activity page (towards the right) when you hover over one of the rows, you will then see the tiny download arrow

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: C

C is correct. Verified through the console

upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

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

Community vote distribution

A (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A. Checked in the docs
upvoted 2 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

A. checked in the docs
upvoted 1 times

🗳️ 👤 **MSKid** 11 months ago

Selected Answer: A

yup course slides, A
upvoted 1 times

🗳️ 👤 **LGlif**e 1 year ago

Selected Answer: A

It is 100% A
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

A is correct. Checked from documentation and course slides.
upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: A

A is the answer. Checked on dashboard
upvoted 2 times

What is the maximum number of patterns that can be added when creating a new exclusion?

A. 10

B. 0

C. 1

D. 5

Correct Answer: C

Community vote distribution

C (100%)

🗳️ **hussainuch** 4 months, 3 weeks ago

Selected Answer: C

upvoted 1 times

🗳️ **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

c. tested in UI and can only add 1

upvoted 1 times

🗳️ **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 2 times

🗳️ **bbqsauceomg** 1 year, 1 month ago

Selected Answer: C

double checked and C is the answer. only 1

upvoted 2 times

🗳️ **Jek88** 1 year, 2 months ago

Selected Answer: C

C is the correct answer, one pattern per exclusion for both ML and sensor visibility exclusions.

upvoted 3 times

🗳️ **Reddington0214** 1 year, 2 months ago

so you think its 0 or no max pattern?

upvoted 1 times

🗳️ **Roy_So** 1 year, 2 months ago

I tried more than 10 patterns, still works

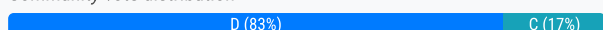
upvoted 1 times

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

Correct Answer: D

Community vote distribution



🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: D

D is the only answer. Also checked in the console
upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: D

D is the correct answer, tested in console.

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.

upvoted 2 times

🗳️ 👤 **bbqsauceomg** 1 year, 1 month ago

answer should be D

here is what it does

Machine-Learning Prevention Monitoring

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).

upvoted 2 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: D

D is the correct answer.

upvoted 2 times

🗳️ 👤 **VJJjo** 1 year, 2 months ago

D IS CORRECT

upvoted 3 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: C

Only Machine-Learning Prevention Monitoring.

upvoted 1 times

🗳️ 👤 **shemilandia** 1 year, 3 months ago

I asked chatGPT "explain me Prevention Policy Debug dashboard reports on CrowdStrike console"

a/ It displays data on events that triggered security policies, such as blocked and allowed events, and the specific policy rule that was applied. This report allows administrators to evaluate the effectiveness of their security policies and make adjustments as necessary to improve the platform's overall security posture.

upvoted 1 times

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

Community vote distribution

B (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **Joe_Kwok** 11 months, 2 weeks ago

Should be "Sensor version updates off" and "Uninstall and maintenance protection turned on"

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

B is correct. Non auto update for being manual. And bulk must be enabled for protection.

upvoted 1 times

🗳️ 👤 **Reddington0214** 1 year, 3 months ago

I think B is the correct answer

upvoted 2 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

B is correct.

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

Tested this in the UI A is correct

upvoted 1 times

🗳️ 👤 **sbag0024** 10 months, 3 weeks ago

What type of Exclusions? ML is only Hosts, IOA is everything. This could be A or B

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: A

A is correct

upvoted 2 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: A

A correct.

First step groups and second everythig else about SVE, and ML. About IOA already dal first step you can change everything.

So you can vhang everything for every exclusion.

upvoted 2 times

🗳️ 👤 **Prr0** 1 year, 1 month ago

A is correct, checked in Falcon

upvoted 2 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

B is incorrect. the exclusion is based on the group, it needs to set the group first.

upvoted 2 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

A correct.

First step groups and second everythig else about SVE, and ML. About IOA already dal first step you can change everything.

So you can vhang everything for every exclusion.

upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: A

A is correct.

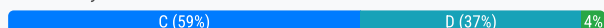
upvoted 4 times

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 offline protection
- D. Identification and analysis of unknown executables

Correct Answer: C

Community vote distribution



EA88 1 month, 1 week ago

Selected Answer: C

Sensor-based Machine Learning (ML) in CrowdStrike Falcon leverages machine learning capabilities directly on the endpoint, allowing the Falcon sensor to provide real-time protection even when the endpoint is offline (i.e., not connected to the internet). This offline protection is a key feature of sensor-based ML, as it enables the detection and blocking of malicious activities locally on the endpoint, without needing constant communication with the cloud.

upvoted 1 times

evilCorpBot7494 4 months, 4 weeks ago

Selected Answer: D

The unknown executables and zero days is the whole purpose of applying Machine Learning to threat detection in cybersecurity. Offline protection should still be had by all modules, otherwise CS would be a very bad solution if it only protects from your blacklisted hashes when you have internet. Answer is D.

upvoted 1 times

sadevek 9 months, 4 weeks ago

In the prevention policy its clearly mentioned that " FOR OFFLINE AND ONLINE HOSTS" - "For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware.", so the answer should be D

upvoted 1 times

Brian9296 1 year, 6 months ago

Selected Answer: D

It's mentioned in the console, "For offline and online hosts.....". So the answer shouldn't be "C".

=====

Sensor Anti-malware

For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware. About levels

upvoted 2 times

DarkieCopy 1 year, 9 months ago

Selected Answer: D

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 offline.

Therefore it is D. Sensor-based ML does not run on hosts when they are offline, discarding C.

upvoted 1 times

TommyJ111 1 year, 10 months ago

Selected Answer: D

D is correct. Says right in the setting "...use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware.

upvoted 1 times

🗨️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

C is correct as it is for offline

upvoted 2 times

🗨️ 👤 **sbag0024** 1 year, 10 months ago

Selected Answer: C

Going with C. The policy says " For offline and online hosts"

upvoted 2 times

🗨️ 👤 **LaCubanita** 1 year, 12 months ago

Selected Answer: D

It should be D, the only option within the Sensor Machine Learning section is Sensor Anti-malware (Detection & Prevention) and it reads: "For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware.

That's basically what option D is

upvoted 2 times

🗨️ 👤 **FerbOP** 2 years ago

Selected Answer: C

C is correct

upvoted 3 times

🗨️ 👤 **Dave071** 2 years ago

Answer is D.

"For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware."

upvoted 1 times

🗨️ 👤 **Prr0** 2 years, 1 month ago

C is correct, check falcon console > Next-Gen Antivirus, Sensor Machine Learning only appear Sensor Anti-malware

upvoted 2 times

🗨️ 👤 **bbqsauceomg** 2 years, 1 month ago

Selected Answer: C

only sensor base include offline

Sensor Anti-malware

For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware. About levels

upvoted 4 times

🗨️ 👤 **testmailuc** 2 years, 1 month ago

Selected Answer: D

I would go with D. After checking the documentation i found this "or unknown and zero-day threats, Falcon applies IOA detection, using machine learning techniques to build predictive models that can detect never-before-seen malicious activities with high accuracy."

ChatGPT also confirms it and some online resources

upvoted 1 times

🗨️ 👤 **andreiushu** 2 years, 2 months ago

Selected Answer: D

For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware

upvoted 2 times

🗨️ 👤 **Roy_So** 2 years, 2 months ago

Selected Answer: C

Correct should be C after revisit the doc.

Provides machine learning-based on-sensor AV protection for malicious files, including offline protection.

upvoted 4 times

  **VJJjo** 2 years, 2 months ago

C should be correct

upvoted 4 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **swapnil1111** 4 months, 3 weeks ago

C is correct.

upvoted 1 times

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

C is correct, tested in the UI

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: C

C is correct

upvoted 2 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

C is the correct. Verified through the console

upvoted 2 times

🗲️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: C

C is the correct answer.

upvoted 3 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **FerbOP** 6 months ago

B is correct

upvoted 1 times

🗲️ 👤 **testmailuc** 7 months, 4 weeks ago

Selected Answer: B

B is correct. verified through the console

upvoted 1 times

🗲️ 👤 **Jek88** 8 months, 2 weeks ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

Why is the ability to disable detections helpful?

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

Correct Answer: A

Community vote distribution

A (83%)

C (17%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: A

A is correct, it is in the docs
upvoted 2 times

🗳️ 👤 **JSN7117** 10 months, 3 weeks ago

Selected Answer: A

Based on Documentation
upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: A

I Agree, the A option is the correct as the documentation tells.
upvoted 2 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

A is definitely the correct answer. After checking the documentation i found this "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"
upvoted 2 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: C

C is the correct answer.
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

A is definitely the correct answer. After checking the documentation i found this "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"
upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (86%)

14%

🗳️ 👤 **Brian9296** 5 months ago

Selected Answer: A

I vote for "A" as B and C can be found under the "Statistics" tab, while D can be found in the "Event" tab in decimal format.
upvoted 1 times

🗳️ 👤 **joal23** 9 months ago

I disagree. The information "the last time the user's password was set" doesn't appear on the logon activity. The correct is D.
upvoted 2 times

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B tested in the ui
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct.
upvoted 1 times

🗳️ 👤 **Dave071** 1 year ago

Answer is B.
upvoted 1 times

🗳️ 👤 **Belrose** 1 year, 1 month ago

Selected Answer: B

I agree with the B answer.
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 time.
The rest of the options are correct information showed in the report, so they are not right answers for the question because it was formulated in a negative way.
upvoted 1 times

🗳️ 👤 **Prr0** 1 year, 1 month ago

D is correct
upvoted 2 times

🗳️ 👤 **Prr0** 1 year, 1 month ago

You are right B is correct
upvoted 1 times

🗳️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: B

B is the correct answer.
upvoted 3 times

🗳️ 👤 **Prr0** 1 year, 1 month ago

The question is about what not appear in the report and the login time appear

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct, checked in the UI
upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct
upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

It should be B. I used this option to troubleshoot sometimes.
upvoted 1 times

🗳️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: B

B is correct answer.
upvoted 1 times

🗳️ 👤 **Reddington0214** 1 year, 2 months ago

Selected Answer: B

B is possibly Correct
upvoted 2 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗳️ **sbag0024** 10 months, 2 weeks ago

Selected Answer: C

Going with C, Tested in lab but workflows seem to be redone and could be a sequential or parallel dependent on where you put it in the work flow.. Bad question

upvoted 2 times

🗳️ **FerbOP** 1 year ago

Selected Answer: C

Checked C is correct answer

upvoted 1 times

🗳️ **Maharshraval** 1 year ago

CAN YOU PLEASE EXPLAIN WHY its C?

upvoted 1 times

🗳️ **Brian9296** 5 months ago

As C is "parallel" action, no dependency of previous action. Imagine if the previous action failed, then the sequential action will not be execute. And parallel action ensured that the IT team and CISO team able to receive the alert email at the same time.

So "C" should be the most appropriate option.

upvoted 1 times

🗳️ **Dave071** 1 year, 1 month ago

Answer is D. Simply add new email to the existing "Send email" Action.

upvoted 2 times

🗳️ **TommyJ111** 10 months ago

The CISO requests a customized message, so D is wrong.

upvoted 2 times

🗳️ **testmailuc** 1 year, 1 month ago

Selected Answer: C

We did that.in action and we went with option C

upvoted 1 times

🗳️ **andreiuslu** 1 year, 2 months ago

Selected Answer: C

I think it's C

upvoted 2 times

🗳️ **Reddington0214** 1 year, 2 months ago

Selected Answer: C

C is much more correct. What you think?

upvoted 3 times

Which of the following is NOT an available filter on the Hosts Management page?

- A. Hostname
- B. Username
- C. Group
- D. OS Version

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **CyberMacadamia** 7 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗲️ 👤 **swapnil1111** 10 months, 3 weeks ago

B is correct, confirmed in Console

upvoted 1 times

🗲️ 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: B

B is correct, tested in the UI

upvoted 1 times

🗲️ 👤 **FerbOP** 1 year, 6 months ago

Selected Answer: B

B is correct

upvoted 2 times

🗲️ 👤 **testmailuc** 1 year, 7 months ago

Selected Answer: B

B is correct. Verified through the console

upvoted 3 times

🗲️ 👤 **Roy_So** 1 year, 9 months ago

Selected Answer: B

B is correct answer. Checked on dashboard.

upvoted 4 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

I think B is the correct, After experience with the console

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Using glob for machine learning exclusions which excludes fiels or folder.

upvoted 1 times

🗳️ 👤 **Reddington0214** 1 year, 2 months ago

Selected Answer: B

B seems correct.. Any inputs?

upvoted 3 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Yes B is correct. Using glob for machine learning exclusions which excludes fiels or folder.

upvoted 1 times

🗳️ 👤 **testmailuc** 1 year, 1 month ago

Also for me i think B is the correct anwser

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct, checked in the docs
upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct
upvoted 1 times

🗲️ 👤 **testmailuc** 1 year, 1 month ago

Selected Answer: B

B is the way that permissions are set. Did it so many time from the console.
upvoted 1 times

🗲️ 👤 **Jek88** 1 year, 2 months ago

Selected Answer: B

B is the correct answer.
upvoted 2 times

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

Correct Answer: C

Community vote distribution

C (100%)

🗉 👤 **sbag0024** 1 year, 4 months ago

Selected Answer: C

Going with C

upvoted 1 times

🗉 👤 **testmailuc** 1 year, 7 months ago

Selected Answer: C

C is the correct answer. Tested and that command with that specific character does not exist.

upvoted 1 times

🗉 👤 **Jek88** 1 year, 8 months ago

Selected Answer: C

C is the correct answer as this command does not exist.

upvoted 2 times

🗉 👤 **CyberMacadamia** 7 months, 1 week ago

Command does exist. However, it does not display the sensor version installed just states if csagent is installed.

upvoted 1 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **sbag0024** 10 months, 2 weeks ago

Selected Answer: B

B is correct, it is right in the doc and was in the training
upvoted 1 times

🗲️ 👤 **FerbOP** 1 year ago

Selected Answer: B

B is correct, done this manually on mac devices
upvoted 1 times

🗲️ 👤 **Roy_So** 1 year, 2 months ago

Selected Answer: B

Correct Answer is B
upvoted 1 times