# Can Cyber Crucible silently respond to an attack, but not alert/notify me?

# Can Cyber Crucible silently respond to an attack, but not alert/notify me?

Created by  Dennis Underwood, last modified on May 18, 2022

You may find that there are legitimate scenarios where you do not want an application doing something (probably on your machines, but do not need notified every time.

This is a separate situation as to where you need something whitelisted, where no action is taken by Cyber Crucible’s data extortion prevention.

The capability you are looking for is silent automated responses.

# Making an existing automated response silent in the future:

First, go to the Manage Incidents page. We’re changing the name to Manage Responses in the near future.

Second, click on the speaker/volume button as seen below.

4784131.png?width=680
Clicking this button brings up the “Silence Incident” or “Silence Auto-Response” modal.

We have analytics that check whether a response should be silent based on previously selected programs and arguments.

In this case, we see that Adobe runs a web server as part of its software suite, and we do not want any future alerts that the web server was suspended.

(In this case, we inserted malicious javascript into the file that Adobe ran, and Cyber Crucible suspended Adobe’s web server from stealing or encrypting data.)

4784138.png
Click on the “Take me to Silent Responses Page”

There will be a menu up for inserting that specific silence rule, but let’s look at the page first:

5013506.png?width=680
We see here that the rules are based on both the process and the process arguments for an automated response, that should not be included in notification emails or other alerts.

The suspending still happens - just no notification about it.

We see here that the we do not want the Microsoft Edge browser, or the Chrome browser, to be able to run when using those arguments, and wildcards before and after to account for other arguments that are present.

(Security explainer insight: Both browsers run an identical piece of code, that loads the browsers in the background without a window on the screen, in order to scan and read your files behind the scenes. We do not want our web browsers doing that behind our backs!)

Regardless of whether you are creating an entirely pre-emptive silent response rule or not, the same window below (in the next section) is the next step.

# Creating a Silent Response

Here we see both the program path, and the program arguments. Wildcards are allowed, to ensure something like a username or application version number won’t stop your behavioral rule from working.

An example of why wildcards are needed is because, there might be a program on all of your employee desktops that are in a group.

C:\Users\mary\Desktop\runme.exe
C:\Users\joe\Desktop\runme.exe

The solution would be:

C:\Users*\Desktop\runme.exe

5046277.png

Here, we see that we are creating a silent response for the entire TEMPORARY GIRAFFE 2 group, for an Adobe Created Cloud path, and we only want to silence responses that have a specific argument (in this case a file path to a certain javascript file).

There are no unique pieces to the path, like usernames, so we can create the rule as is.

Responses may be named, with the names being unique per group.

The rules start being distributed to agents within minutes.