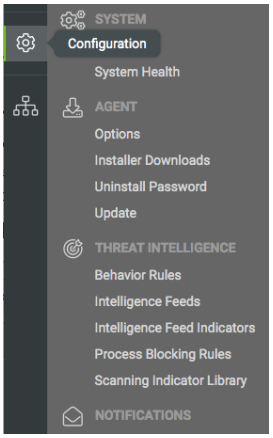
Appendix B – Endpoint Instructions for YaraScab

How to import a YARA ruleset for scanning via “YaraScan” or “ThreatScan”

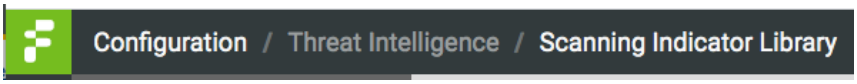
Download the file from: https://github.com/fireeye/sunburst_countermeasures/blob/main/all-yara.yar

NOTE: Keep in mind you can break up the YARA file into smaller groupings to run more efficiently.

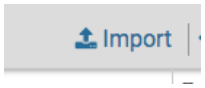
On the Fidelis Endpoint console, visit the **Configuration** page and select Scanning Indicator Library as show below.



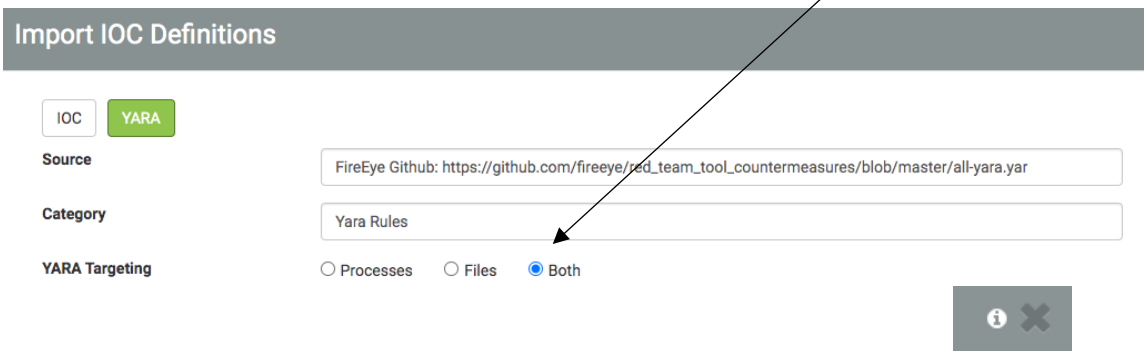
This will bring up the page where you can import the YARA ruleset.



On the right side click **Import**.

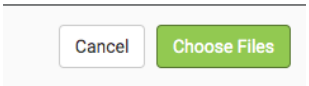


You will then see the option for YARA. Under targeting choose “Both” files and processes.



For additional information about Filtering options see the Help menu by selecting the “i” icon à

Next you will need to choose the file downloaded as a first step in Appendix B.

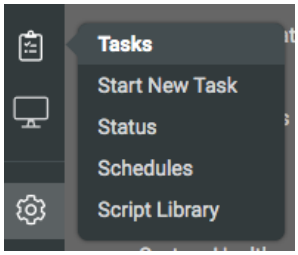


Then Browse Files (top right) à Select the file à Click Import (bottom right) à Close when completed. Your new Yara package should show up in the list.

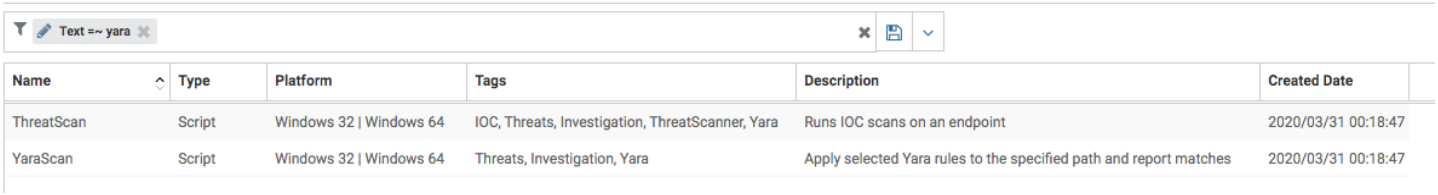
Appendix B – Endpoint Instructions for YaraScab

NOTE: You can also edit and add additional details and a description. Just click the three dots to the left of the package name once imported into your scanning library.

Select the **Tasks** from the menu and choose the **Start New Task** option.



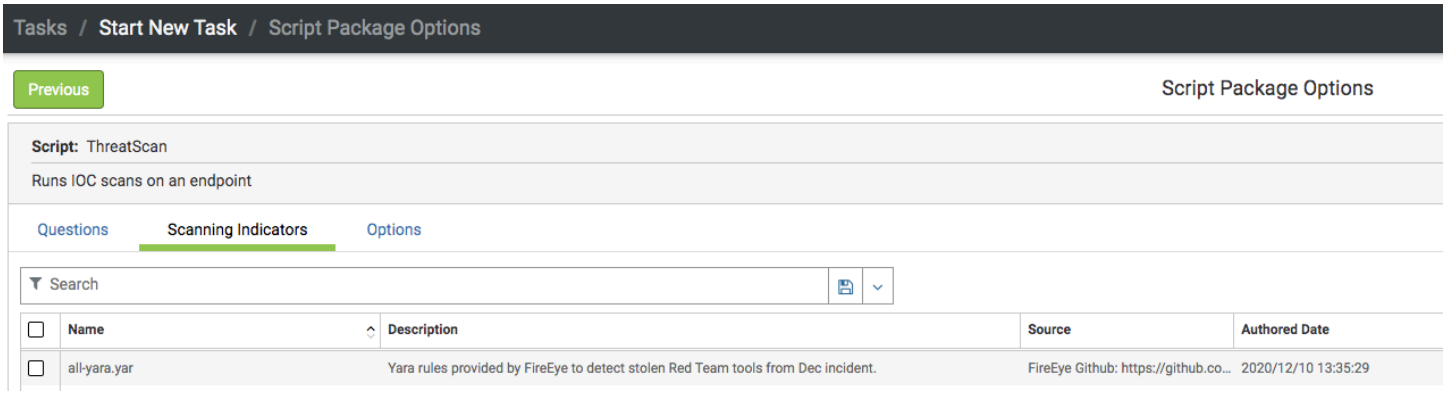
There will be a long list but search for “Yara” in the box and the following options should show up:



ThreatScan – interrogates an endpoint (windows only)

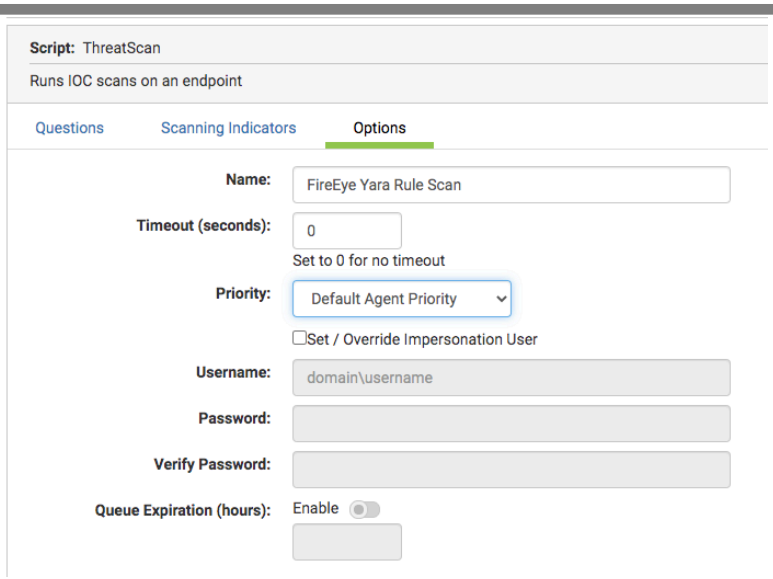
YaraScan – targets a path on the endpoint (windows, linux and mac)

Choose which option is best for you and click **Next** in the top right corner. The next screen should look like this:



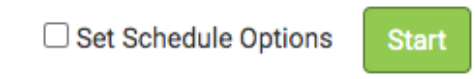
Find the Yara script in the list under **Scanning Indicators** and select it, then click **Next**.

Appendix B – Endpoint Instructions for YaraScab

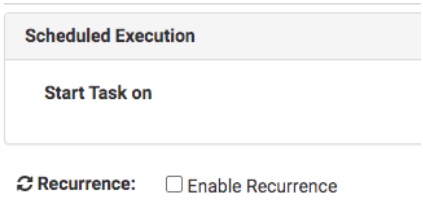


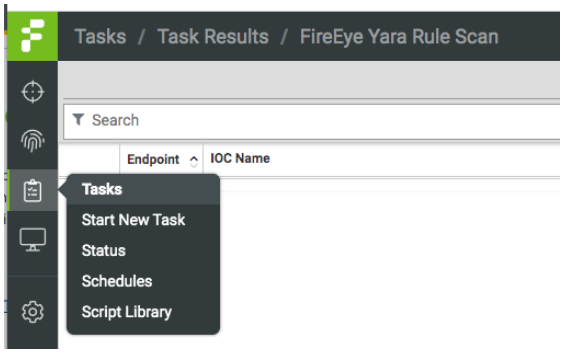
Choose which Targets (endpoints) to run this on by checking the box(es).

In the top right corner, you can either **Start** the job or check the box to **Set Schedule Options**.



Scheduling options allow you to set recurrence enabling this YARA package to be scanned as often as you wish.





You can view the status of your job and results via the **Tasks** menu, just select **Status**.