

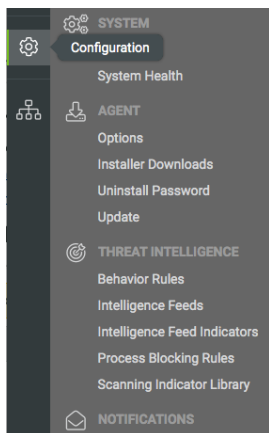
Appendix B – Endpoint Instructions for YaraScab

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

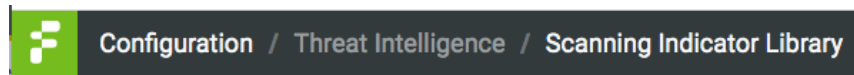
Download the file from: https://github.com/fireeye/sunburst_countermeasures/blob/main/all-yara.yar

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

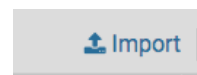
On the Fidelis Endpoint console, visit the **Configuration** page and select Scanning Indicator Library as show below.



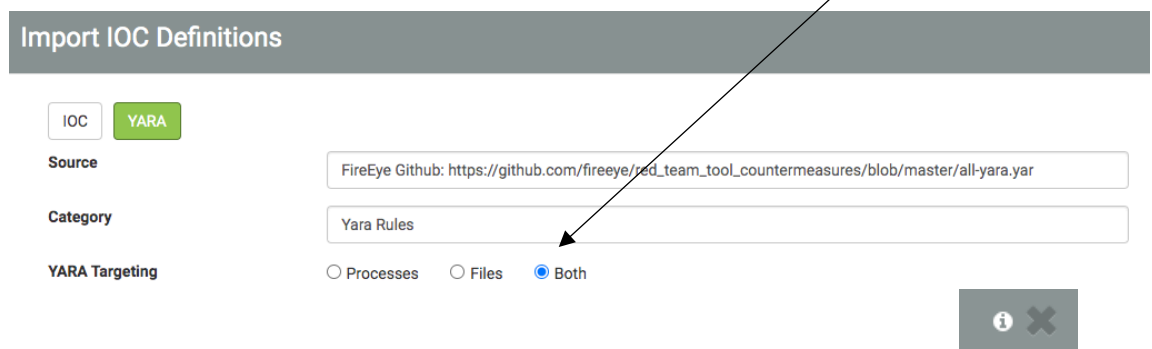
This will bring up the page where you can import the YARA ruleset.



On the right side click **Import**.

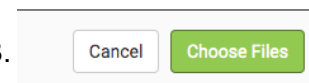


You will then see the option for YARA. Under targeting choose “Both” files and processes.



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.

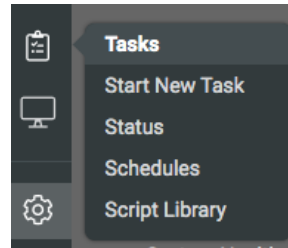


Then Browse Files (top right) à Select the file à Click Import (bottom right) à Close when completed. Your new Yara package should show up in the list.

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:

Name	Type	Platform	Tags	Description	Created Date
ThreatScan	Script	Windows 32 Windows 64	IOC, Threats, Investigation, ThreatScanner, Yara	Runs IOC scans on an endpoint	2020/03/31 00:18:47
YaraScan	Script	Windows 32 Windows 64	Threats, Investigation, Yara	Apply selected Yara rules to the specified path and report matches	2020/03/31 00:18:47

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:

Tasks / Start New Task / Script Package Options

Previous Script Package Options

Script: ThreatScan
Runs IOC scans on an endpoint

Questions Scanning Indicators Options

Search

<input type="checkbox"/>	Name	Description	Source	Authored Date
<input type="checkbox"/>	all-yara.yar	Yara rules provided by FireEye to detect stolen Red Team tools from Dec incident.	FireEye Github: https://github.co...	2020/12/10 13:35:29

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

Appendix B – Endpoint Instructions for YaraScab

Script: ThreatScan
Runs IOC scans on an endpoint

Questions Scanning Indicators **Options**

Name: FireEye Yara Rule Scan

Timeout (seconds): 0
Set to 0 for no timeout

Priority: Default Agent Priority

Set / Override Impersonation User

Username: domain\username

Password:

Verify Password:

Queue Expiration (hours): Enable

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**.

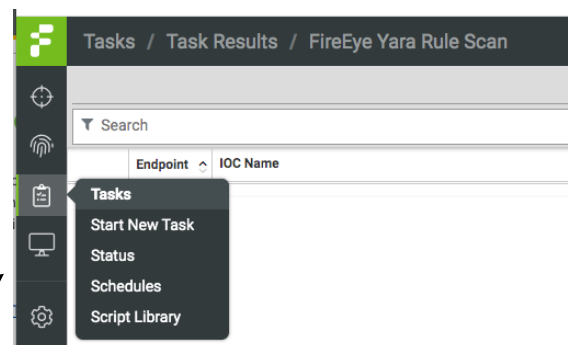
Set Schedule Options **Start**

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

Scheduled Execution

Start Task on

Recurrence: Enable Recurrence



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