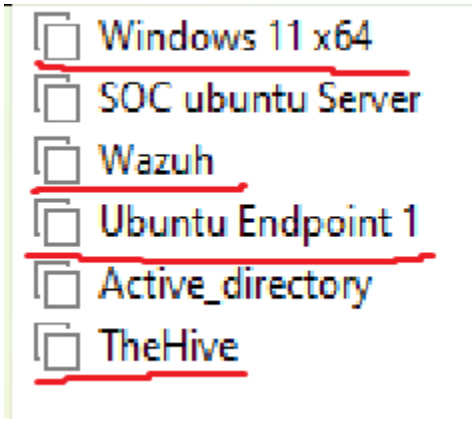
Before starting the installation of Wazuh, I went and created three separate VM's 3 linux, and 1 windows.

You're going to have a Wazuh manager, theHive Case Management, Linux and windows Endpoints. This will give a view on managing two different operating systems utilising Wazuh.



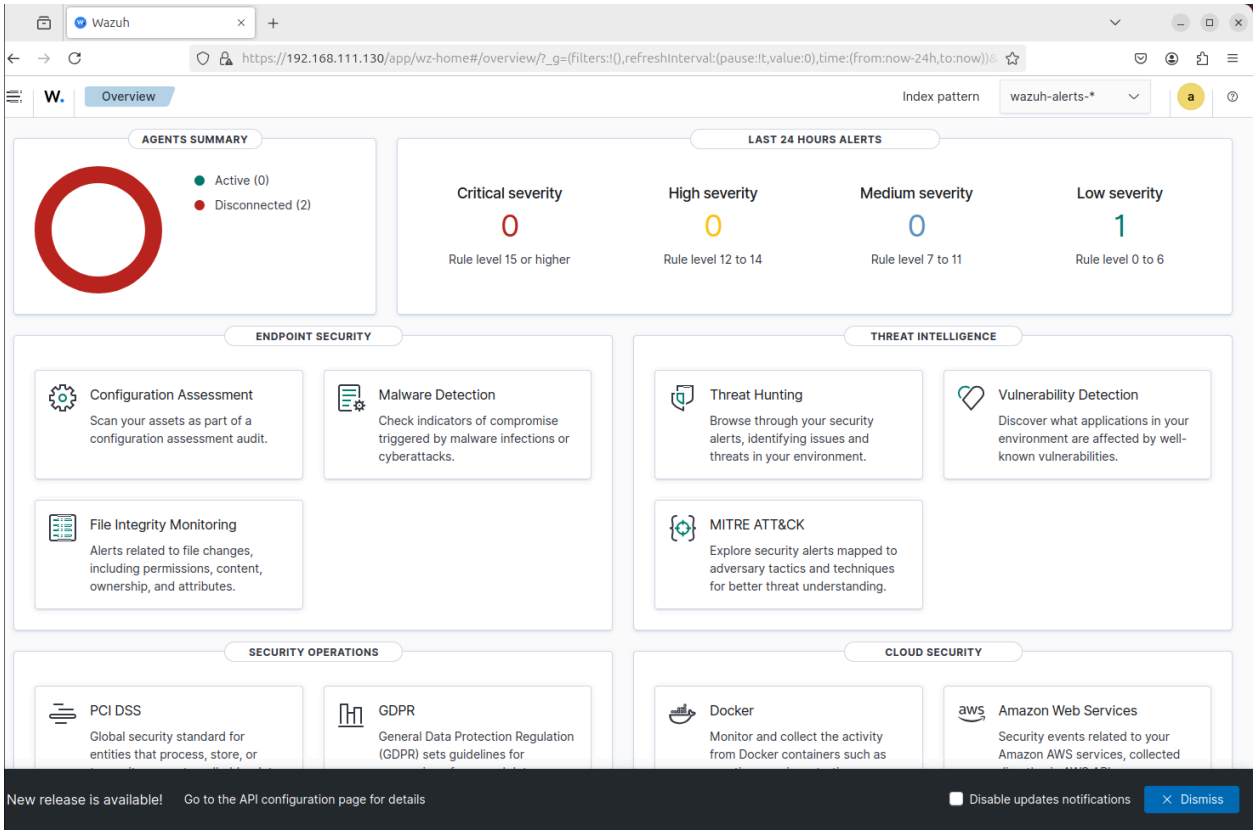
Setting up Wazuh is pretty easy, I've gone with the quickstart installation

https://documentation.wazuh.com/current/quickstart.html

After setting up for the wazuh manager for the linux machine you'll be shown a username and password on the terminal, it'll be something like this.

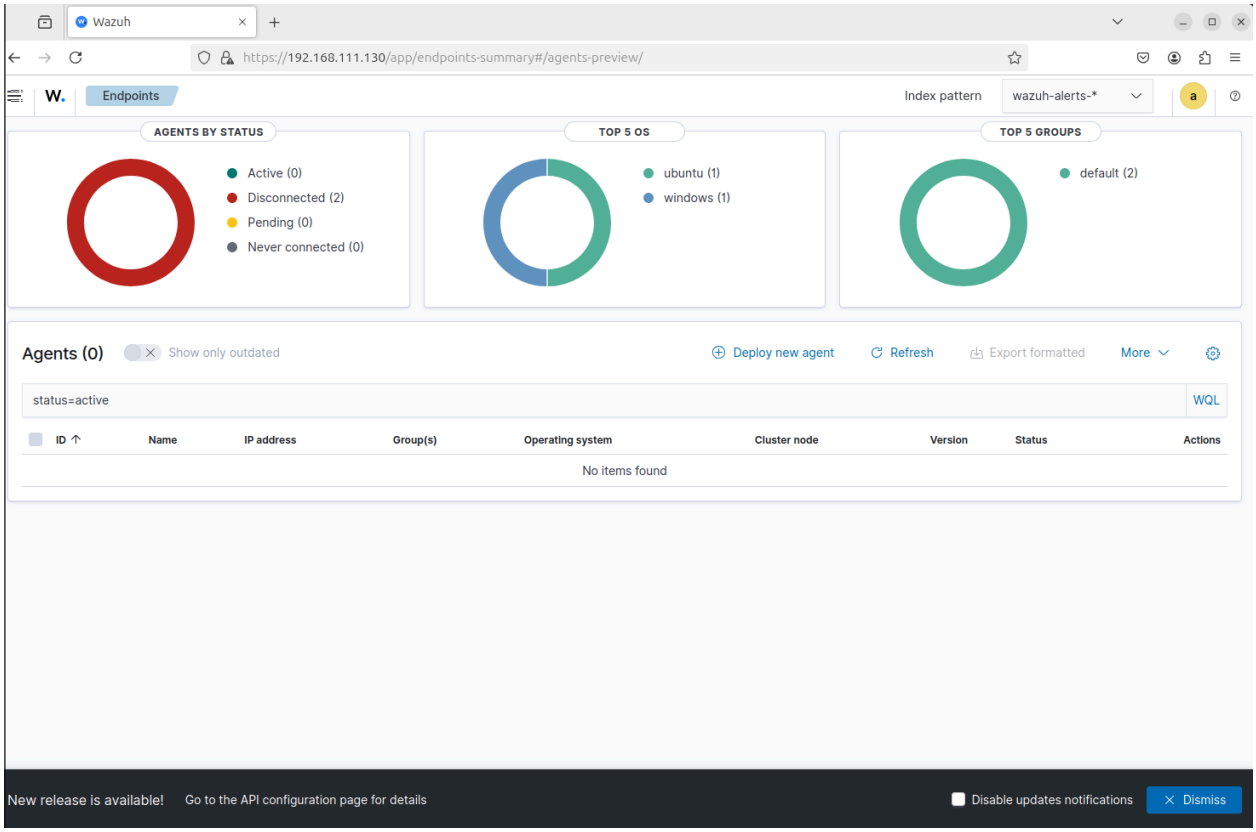
After installation go to wazuh dashboard in your preferred browser, this should be your local IP address which you would find with the command **ip addr**, and it usually the ens33 where you'll find your own IP address, Type this into the URL of your browser and you'll get the Wazuh dashboard if installation of wazuh manager is successful.

Login in with the credentials that was given before on the terminal and you'll be shown the dashboard

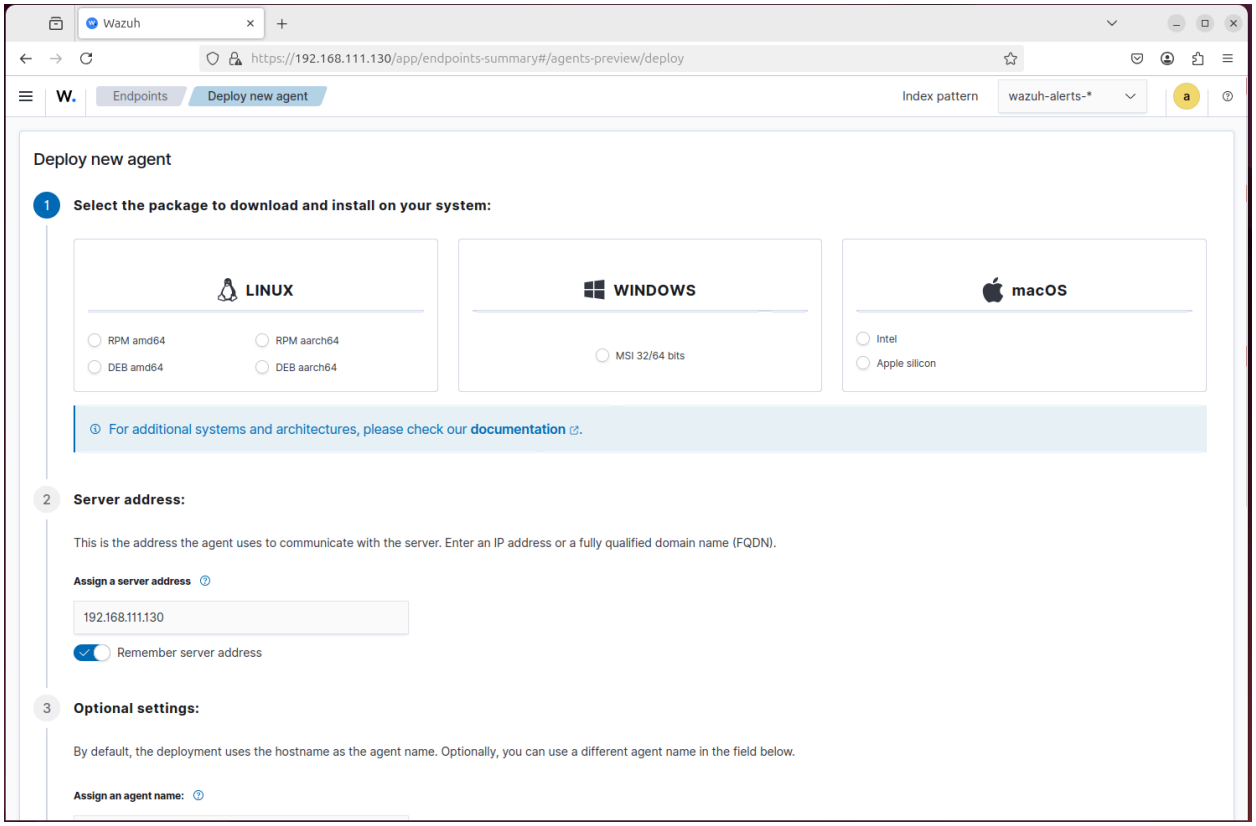


Most of the online tutorials that you use for Wazuh is going to have the old dashboard, it's going to look different and you may need to experiment around but majority of the task utilised in the tutorials will be in the threat Hunting section

Clicking on the agents summary you'll get moved into the endpoints section of wazuh.

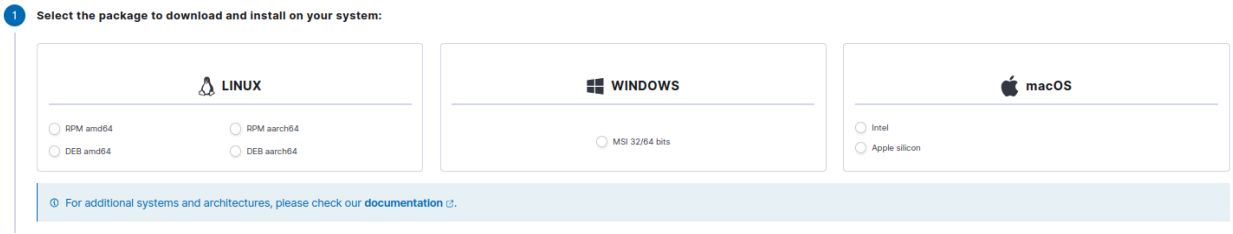


Here is where you'll configure the agent to the specific operating system, so going ahead and clicking on the "deploy new agent"



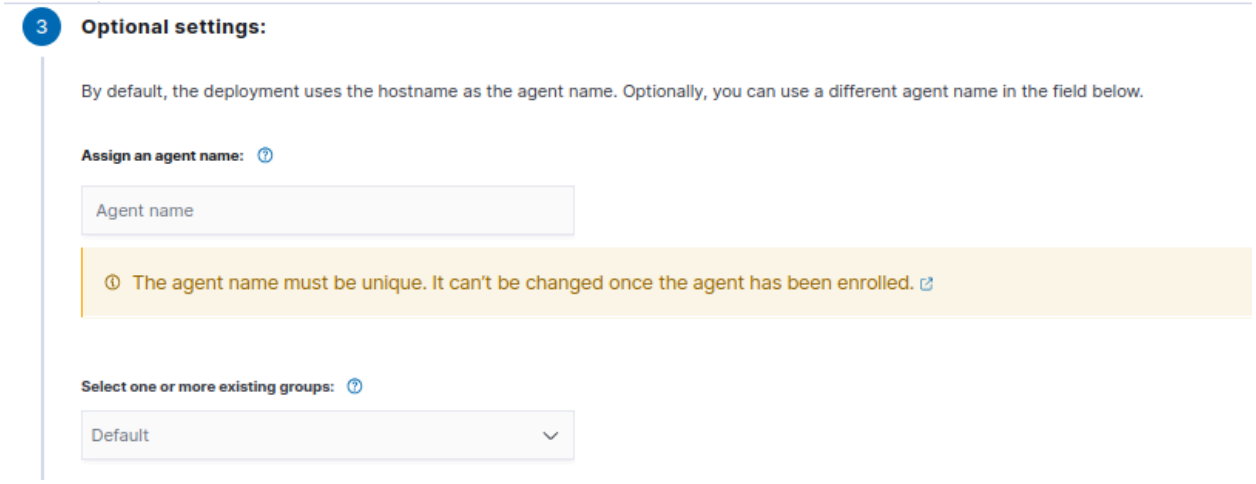
depending upon what operating system you want to install the wazuh agent on, wazuh will have dedicated choices for its specific installation.

You’re going to be prompted with a couple of options

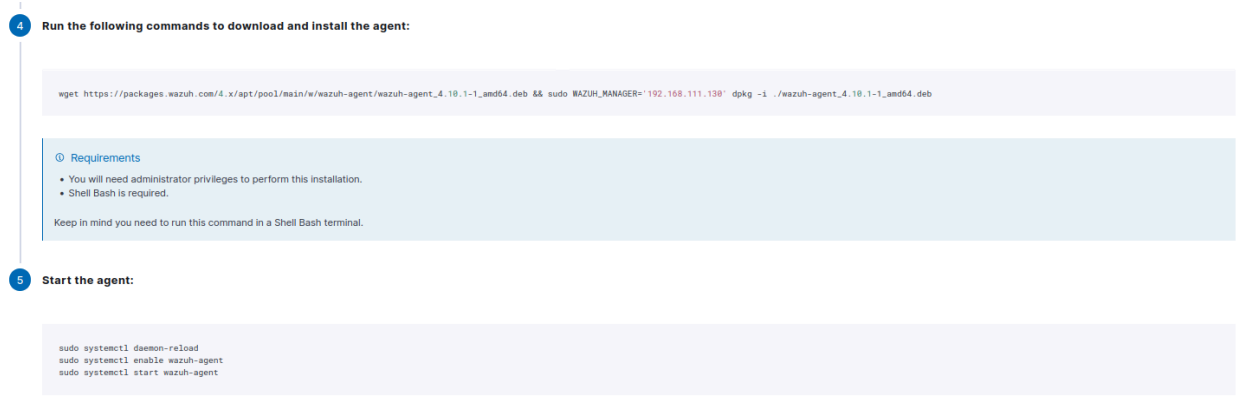


this is for choosing your operating system

Pretty self explanatory, this simply just the IP address the wazuh agent is going to connect to, this should be your main host IP address like the one shown in the image, but the ip will need to be specific to yours



This step is optional but this will be the naming of the wazuh agent, and also the option of grouping it, say for example you have a large network of operating systems that specific to employees, you could put the new wazuh agent you're configuring into this group for better organisation when you need to access said agent.

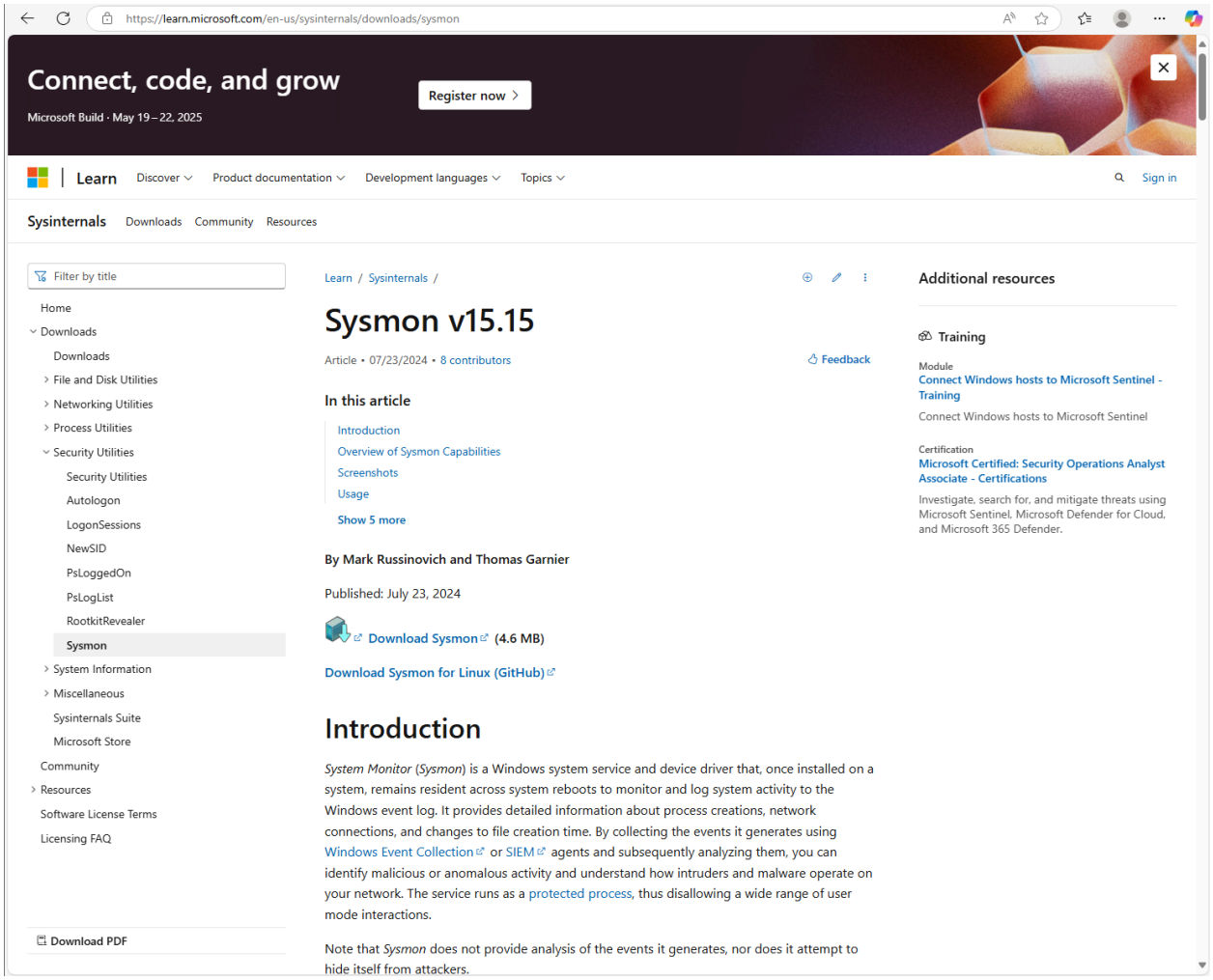


lastly these two steps will be the installation and running of the wazuh agent to the system, you'll paste the commands into the operating system and it should connect to the wazuh manager

Windows

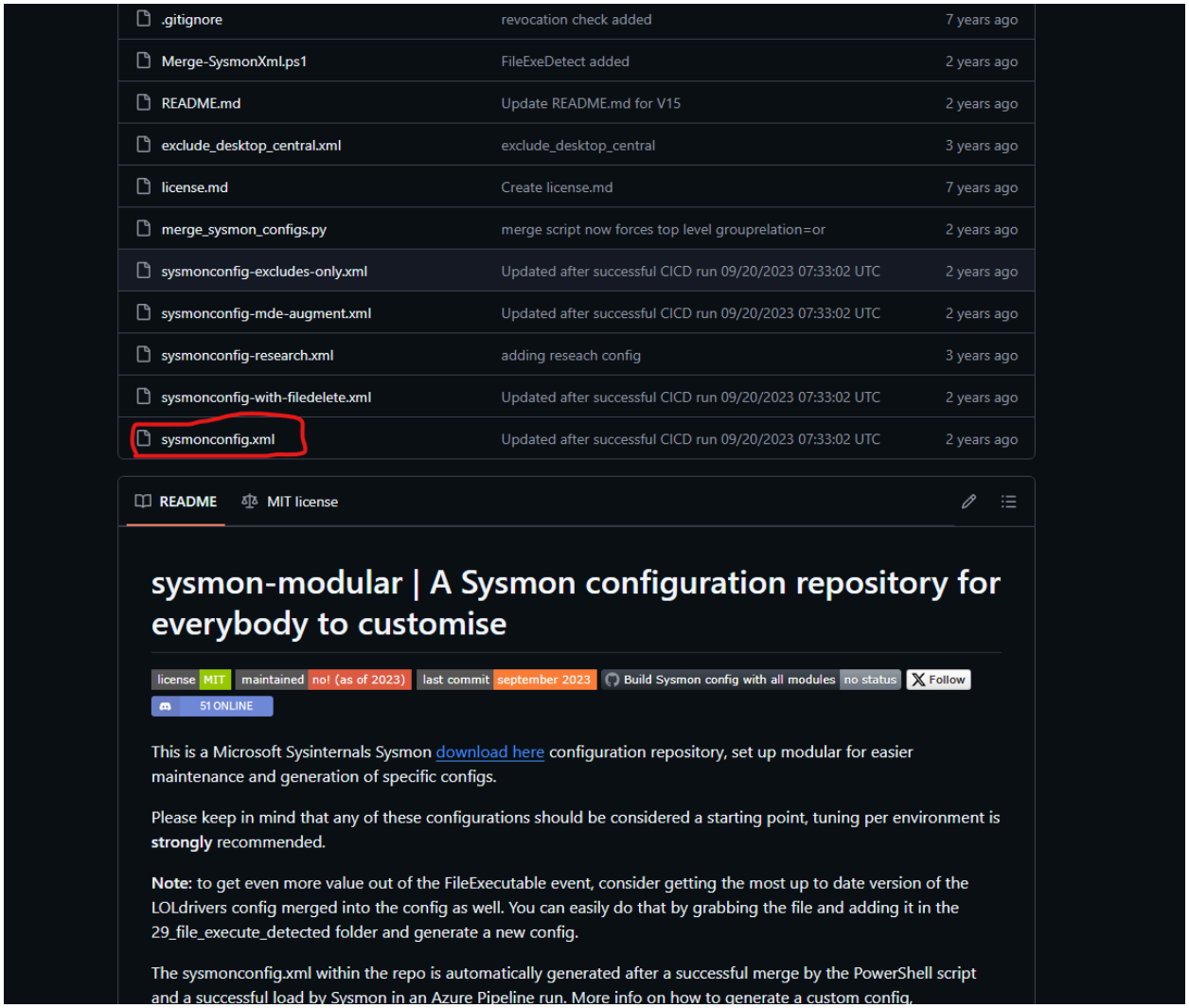
For the windows side of configuration the installation will be about the same, but windows machine out of the package do not come with all the security log collection unless you install it and configure it to detect.

In your windows machine you must search up sysmon, which is a windows specific addon that extends the log collections and monitoring that default windows doesn't come with. installation is pretty easy, just go into sysmon windows and click the download and extract the zip file.

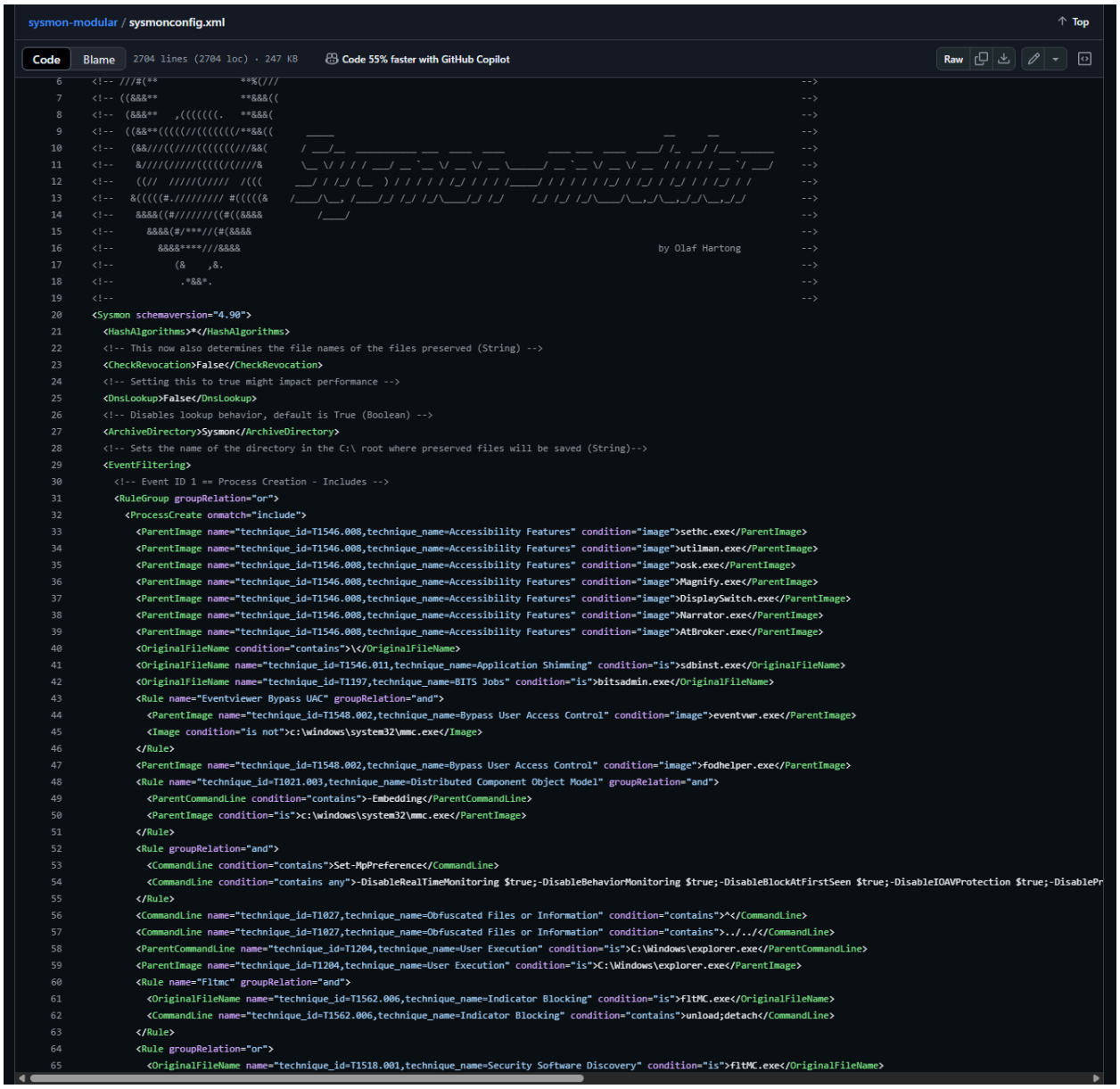


Sysmon also isn't configured but can be through adding additional rules. A great pre-made configuration by olafhartong - sysmon modular (https://github.com/olafhartong/sysmon-modular

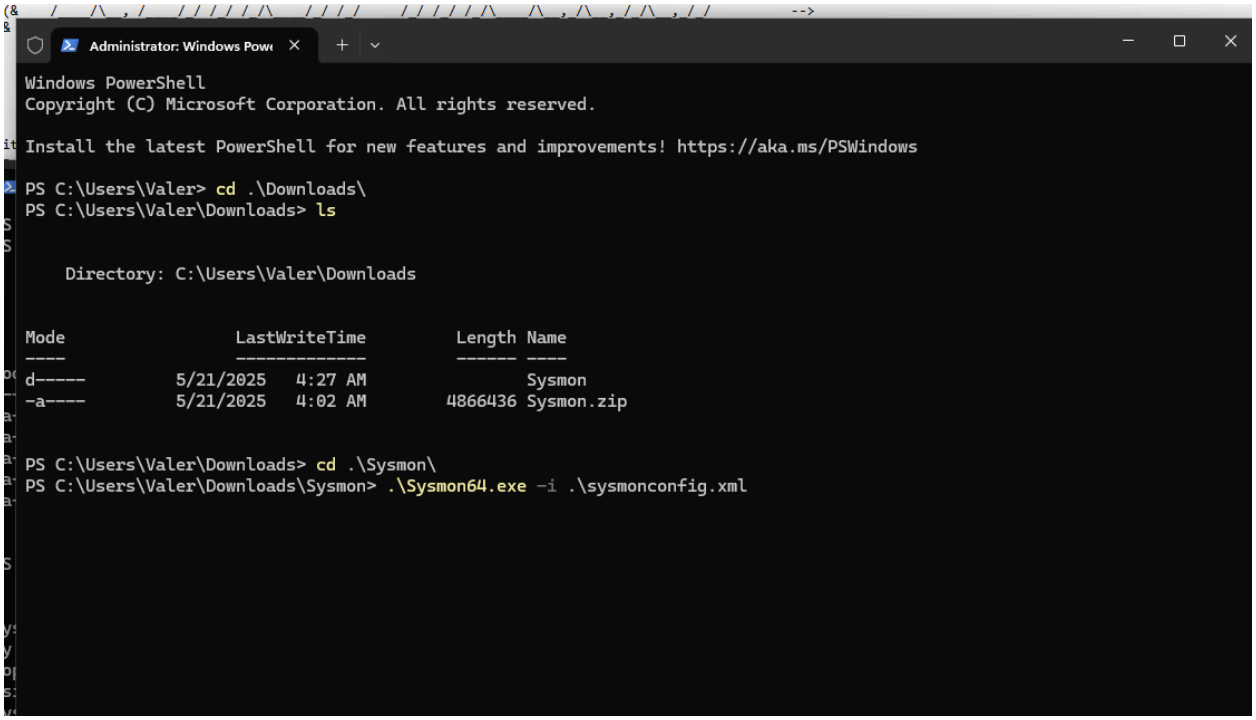
). By scrolling down and finding the sysmonconfig.xml file



You'll get this beautiful config file in which you'll need to save the raw file of this config to be inserted into your windows sysmon, as said by the creator of the github, the sysmon config he created is just a starting point and should be fine tuned to the environment you are using as there are many blindspots or areas he decided not to look into.

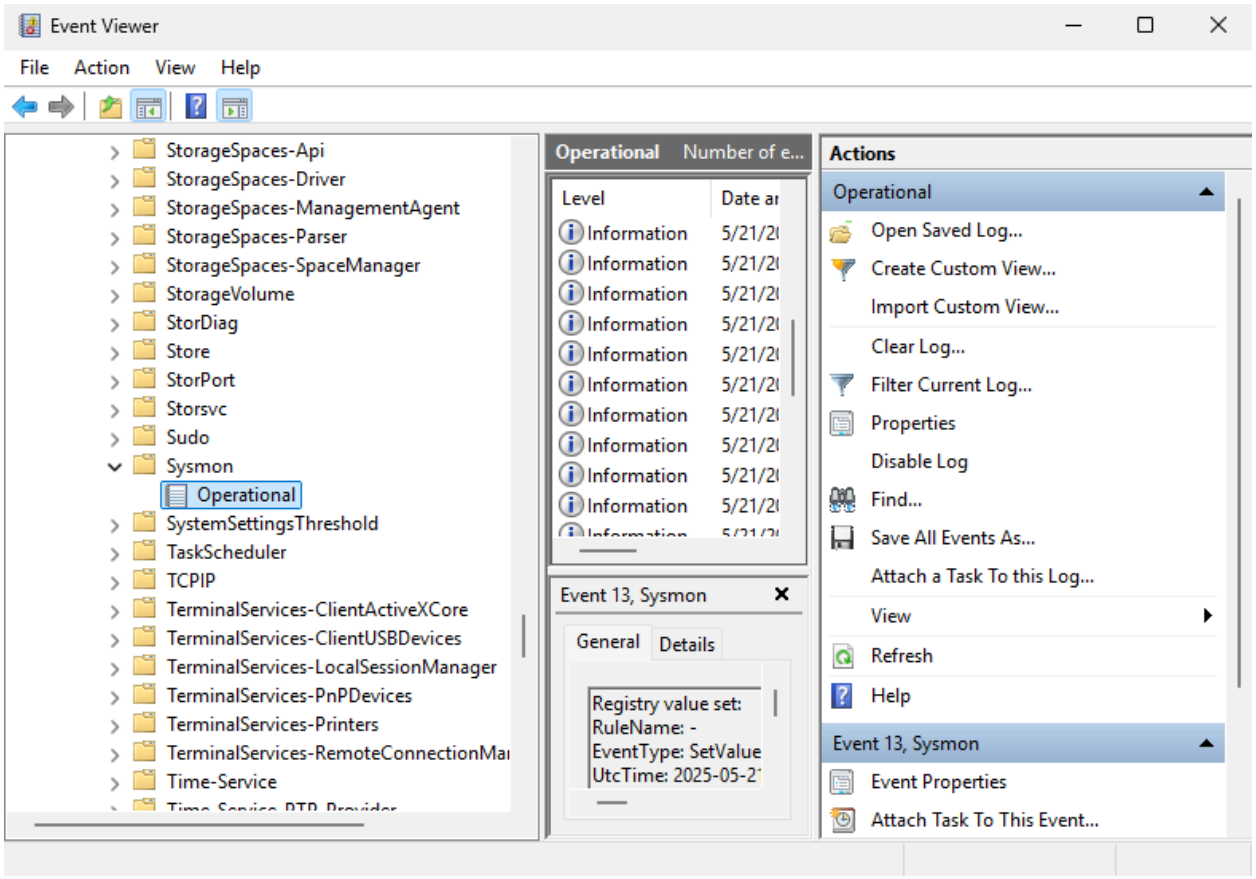


After saving this, it should be saved in the Downloads section of your windows machine. Remember this path because you'll need to access the location of the two files within powershell



I'm going to assume you understand the difference between relative and absolute path, but for easy of use cause I'm lazy, I manually put the sysmonconfig.xml file in the sysmon folder because I wasn't bothered typing the entire path. But through this it'll tell sysmon to use this configuration, if done currently you'll be prompted by a EULA and it'll install. To confirm the service is running run event viewer on windows

event viewer > Applications and services log > Microsoft > Sysmon



Troubleshooting.

There is a problem with the sca scan not showing anything

The Sca scan would be found where the **image before,** if there is nothing being shown like the image above. This could possibly be the configuration on the wazuh agent end, as wazuh needs

the precise operating. The solution is found by Wesly Khanh
https://groups.google.com/g/wazuh/c/cUjIf6g01Vk

By going onto the wazuh agent operating system which mine is going to be linux, but the file is the same as windows so this problem will occur if the specific operating system for windows isn't the same as describe for example, the configuration file has windows 11 pro instead of windows 11 home

```
root@endpoint-1-VMware-Virtual-Platform:/var/ossec/ruleset/sca# pwd
/var/ossec/ruleset/sca
```

so having root access you want to go to this command **/var/ossec/ruleset/sca**

```
root@endpoint-1-VMware-Virtual-Platform:/var/ossec/ruleset/sca# ls
cis_ubuntu22-04.yml
```

once you ls you'll see the specific yaml file that is installed when you installed the wazuh agent, you'll want to edit this file with your choice of editor.

```
20 requirements:
21   title: "Check Ubuntu version."
22   description: "Requirements for running the SCA scan against Ubuntu Linux 22.04 LTS"
23   condition: all
24   rules:
25     - "f:/etc/os-release -> r:Ubuntu 24.04"
26     - "f:/proc/sys/kernel/ostype -> Linux"
27
```

On line 25, you'll want to change the os-release to your specific operating system, in the image above it has been changed already but originally it was **r:Ubuntu 24.02** instead of being **r:Ubuntu 24.04**. After you've made the changes you'll want to restart the wazuh agent with **systemctl restart wazuh-agent**