SYSMON SETUP.

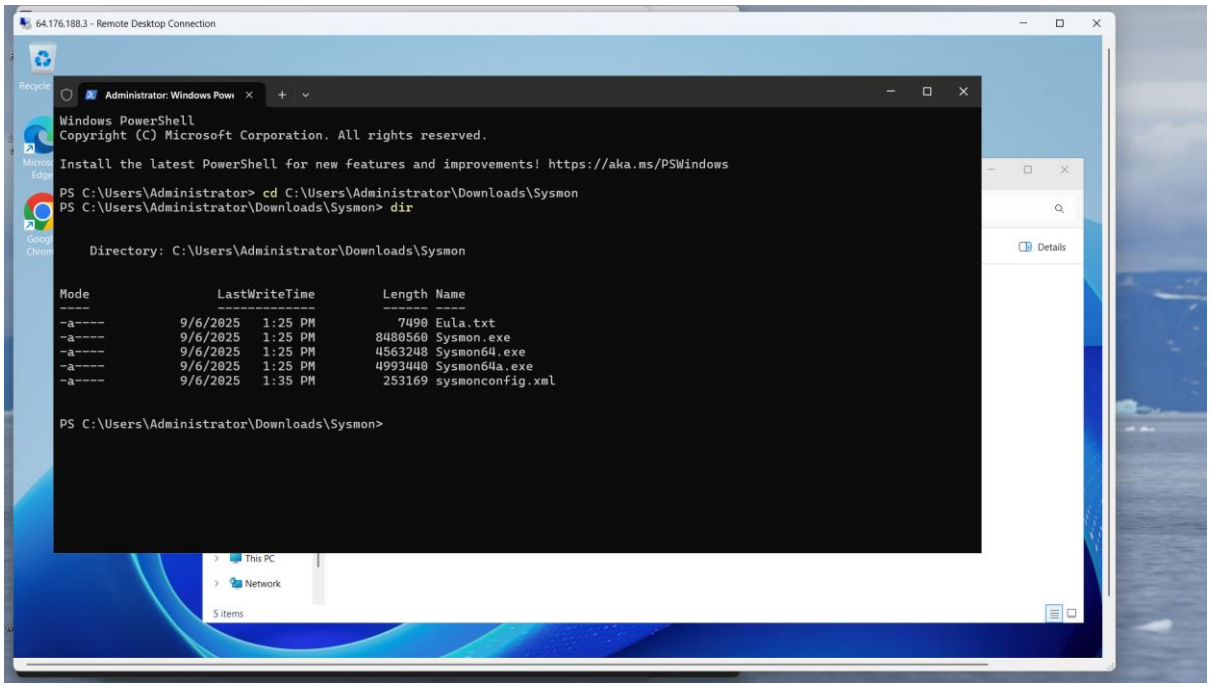
Objective: install and configure sysmon on a windows server.

Tools Used

- Sysmon (Sysmon64.exe) – for monitoring and capturing system activity.
- Sysmon configuration file (sysmonconfig.xml) – defines what events and activities Sysmon records.
- Windows Event Viewer – for validating Sysmon event logs.
- Elasticsearch – for ingesting and analyzing Sysmon and Windows Defender logs.
- Windows Server & PowerShell – for installing, configuring, and managing Sysmon.

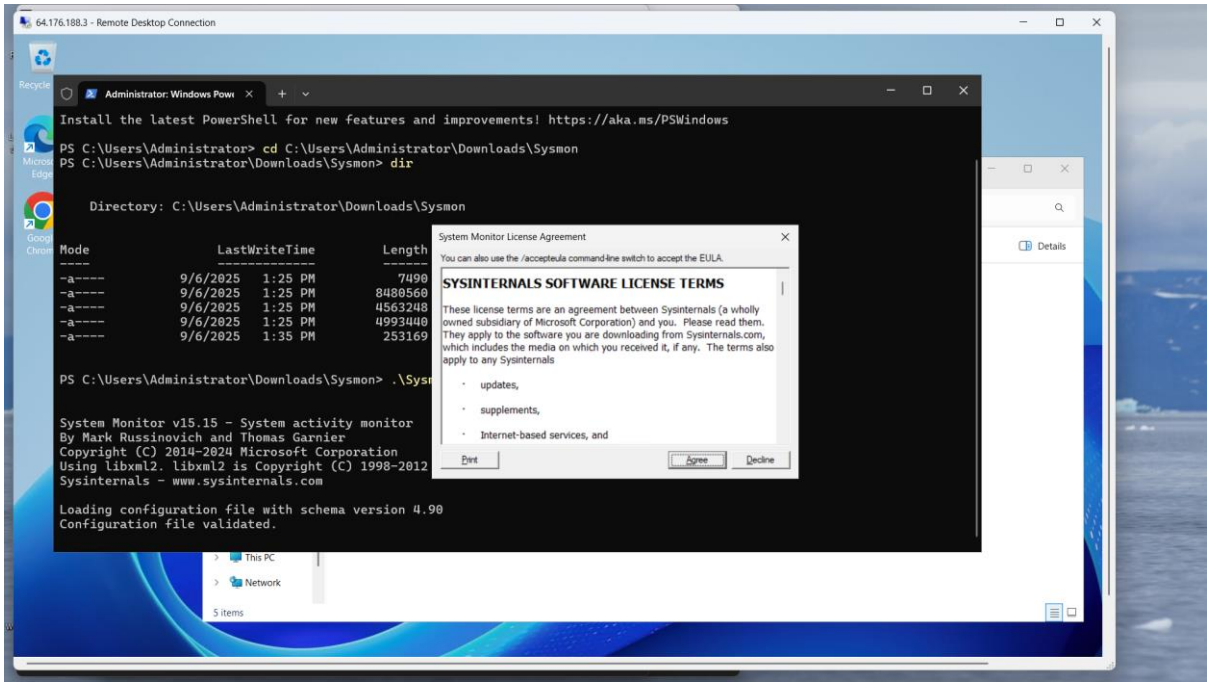
In your windows server, download sysmon and the configuration file **sysmon olaf configuration** on github and then save the **raw** file of **sysmonconfig.xml**.

Open powershell, run as administrator on the windows server and open the sysmon directory to confirm your xml file and the sysmon configurations.

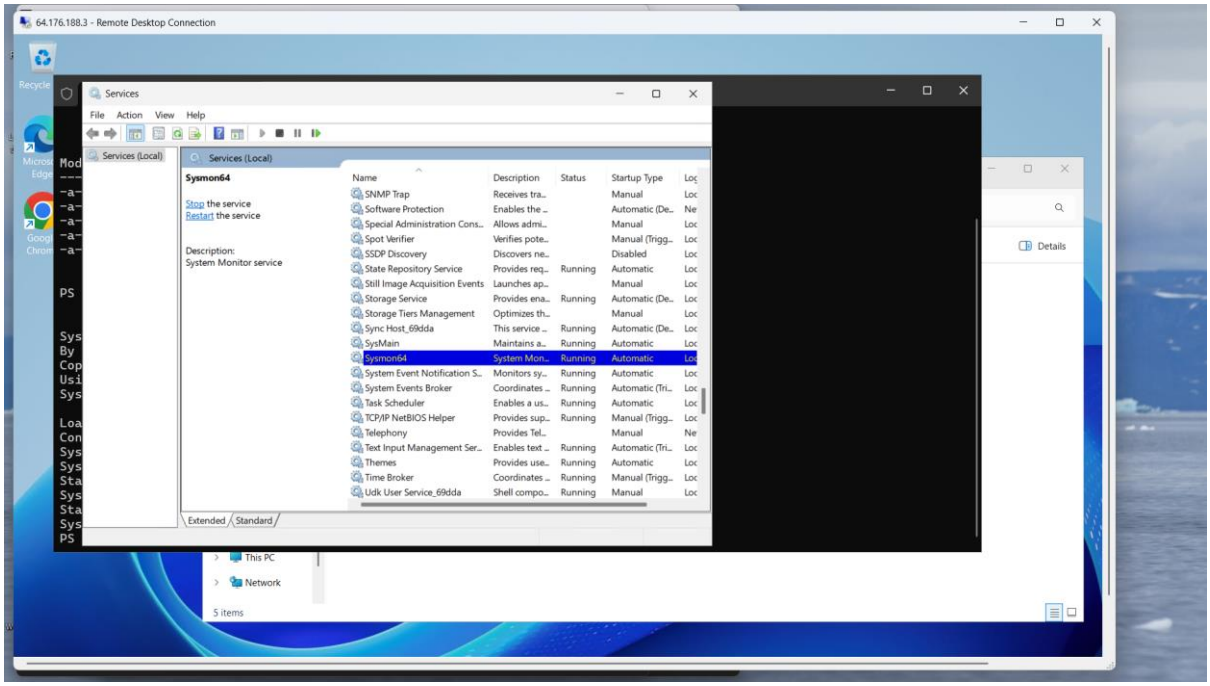


To install sysmon, use the command **.\Sysmon64.exe –i sysmonconfig.xml**

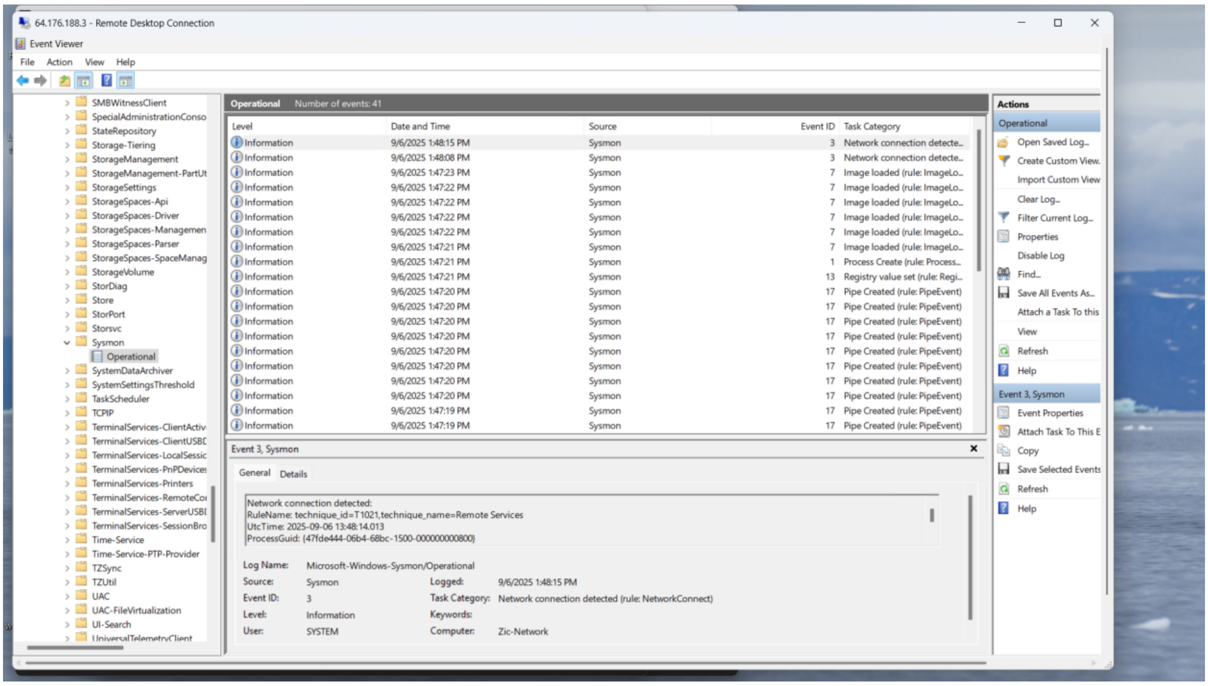
This prompt will bring up a license agreement page to start sysmon installation.



Sysmon should be installed and you can confirm it in your services and the event viewer in your windows server.

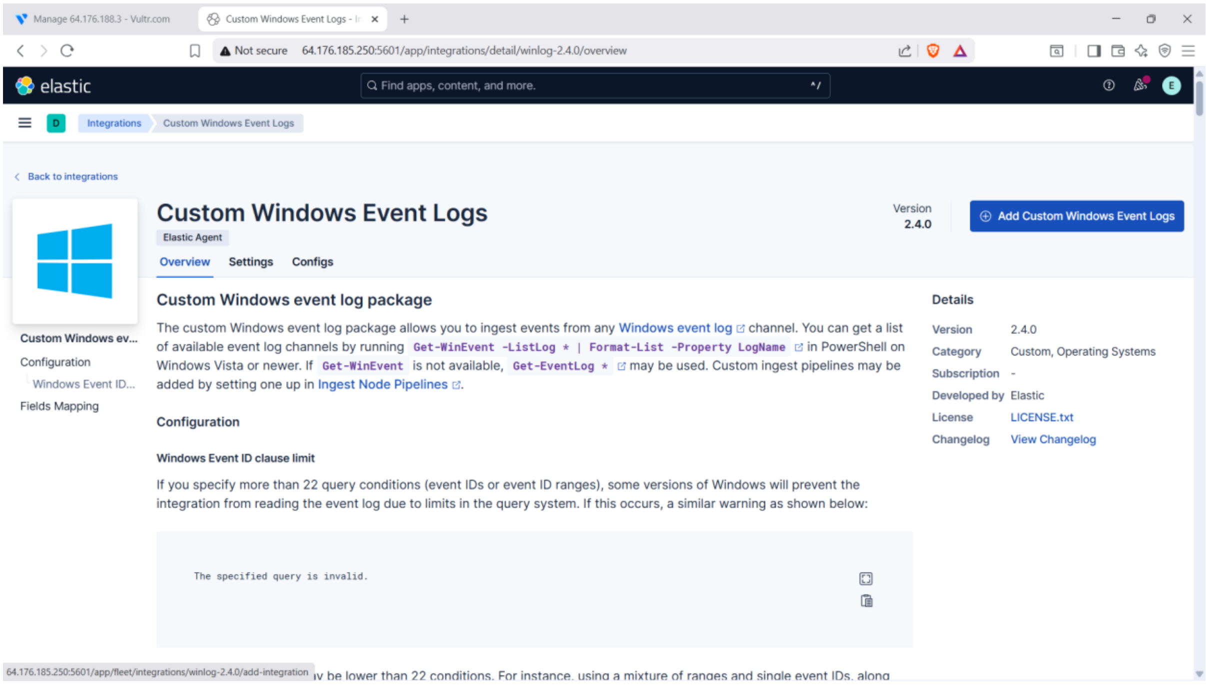


In the event viewer, after expanding the **operational**, we can see an Event ID 3, this captures network connections, Event ID 7 captures image loaded event logs in a specific process, Event ID 1 captures process creation and so on.

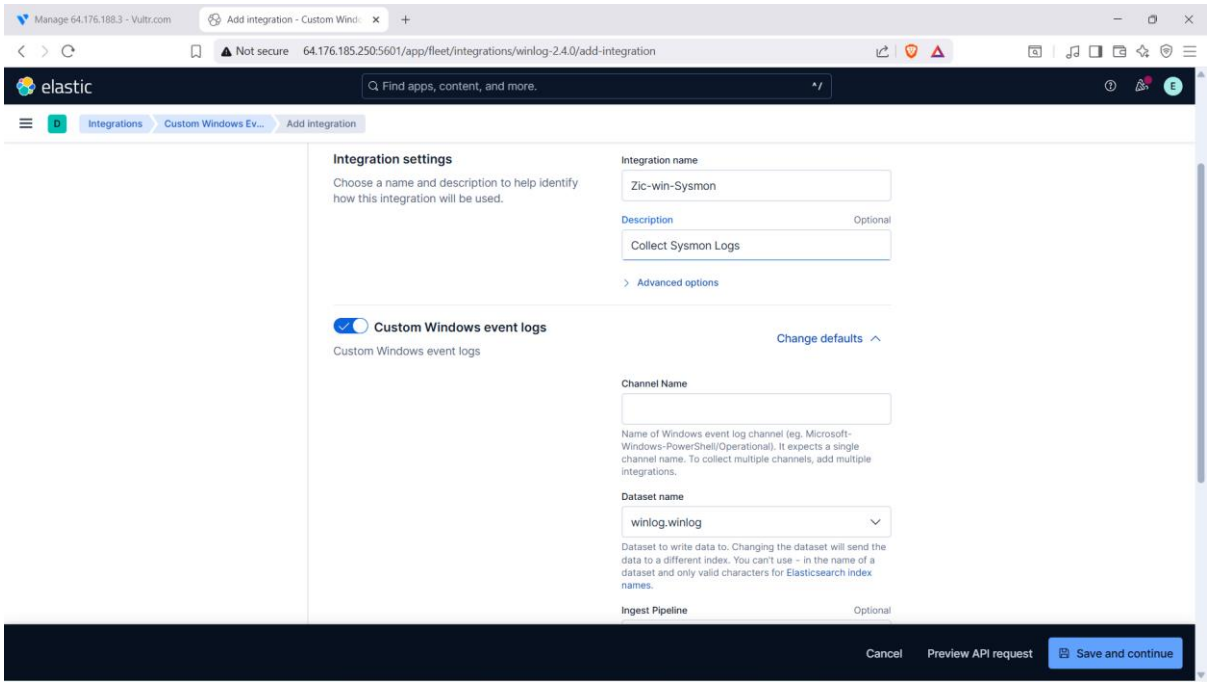


HOW TO INGEST SYSMON AND WINDOWS DEFENDER EVENT LOGS INTO ELASTICSEARCH.

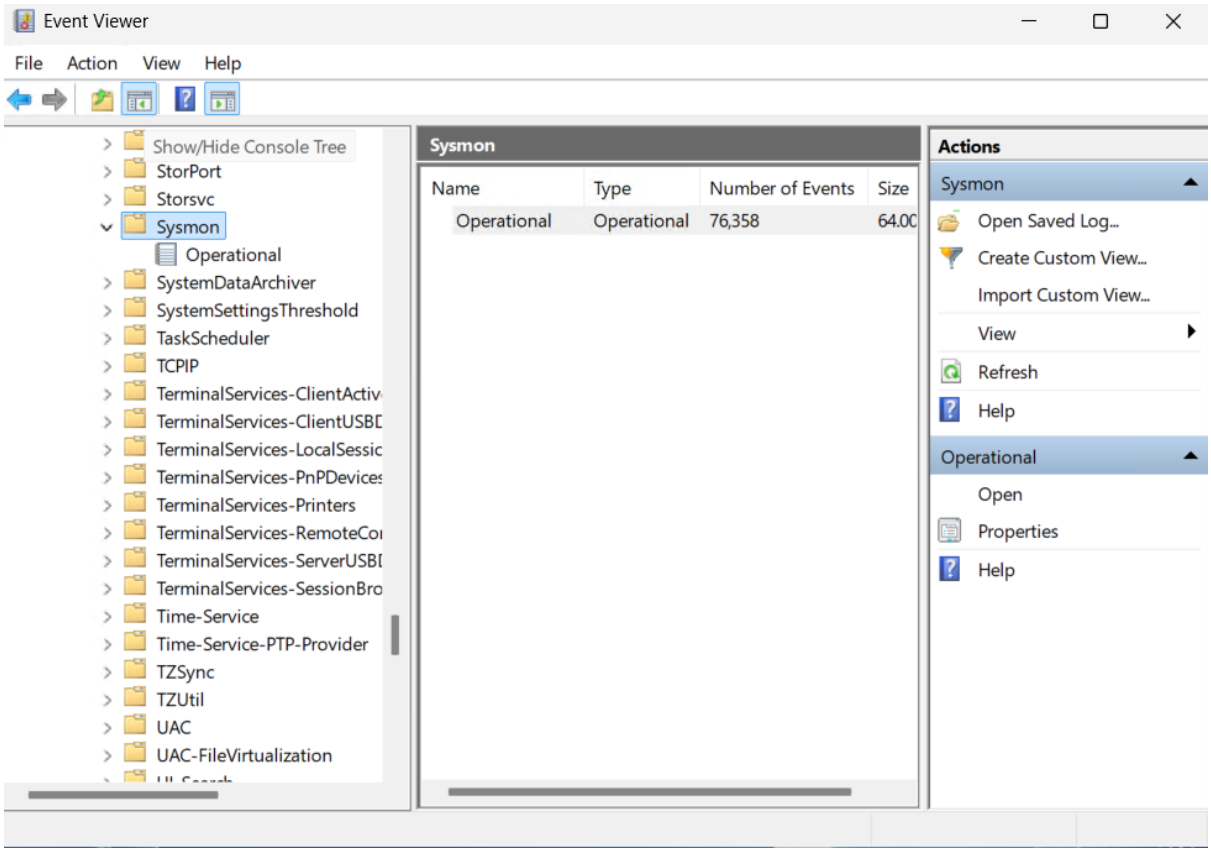
On the homepage of your elasticsearch, select the button **Add integration.** Search up **Custom Windows Event Logs** and click **add custom windows event logs.**



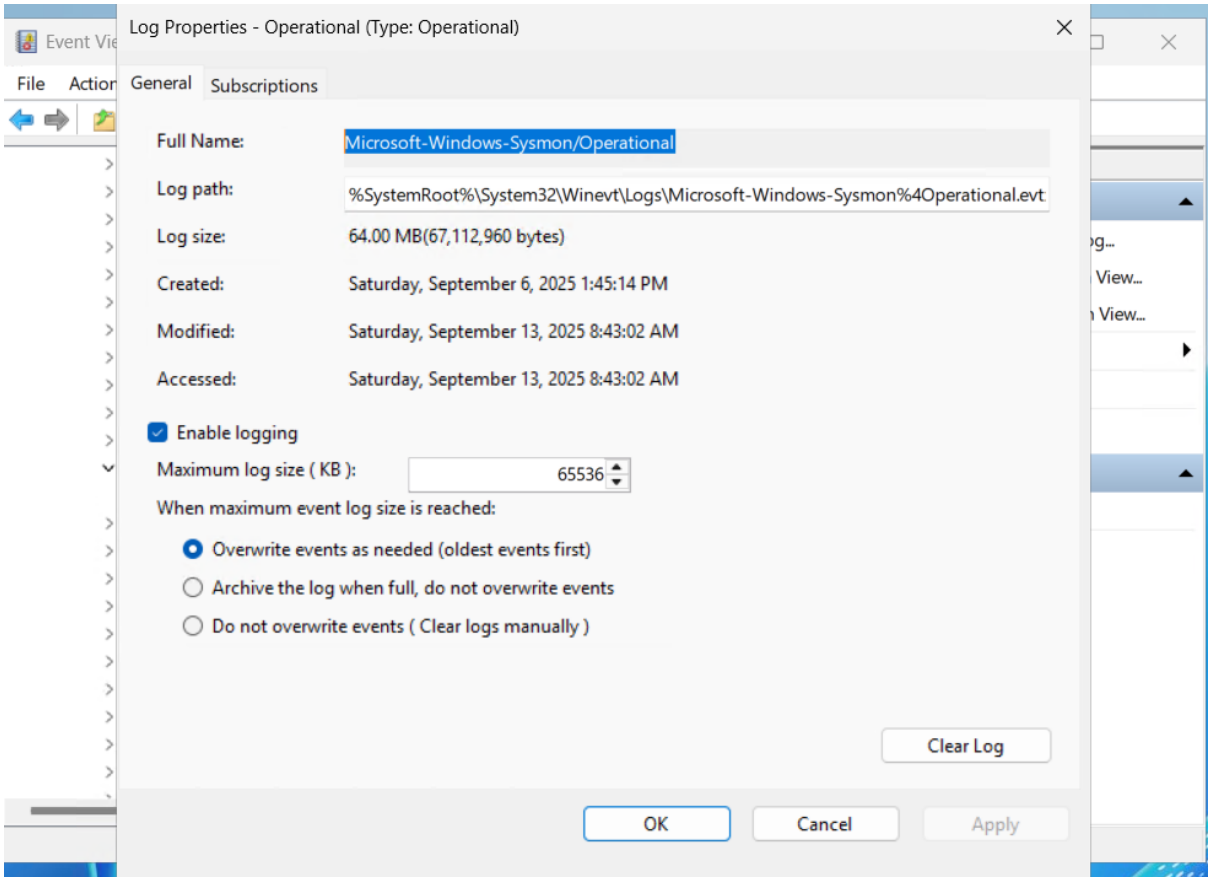
Add the **integration name** and **description,** when it comes to the **custom windows event logs**, the **channel name** is gotten from the windows server.

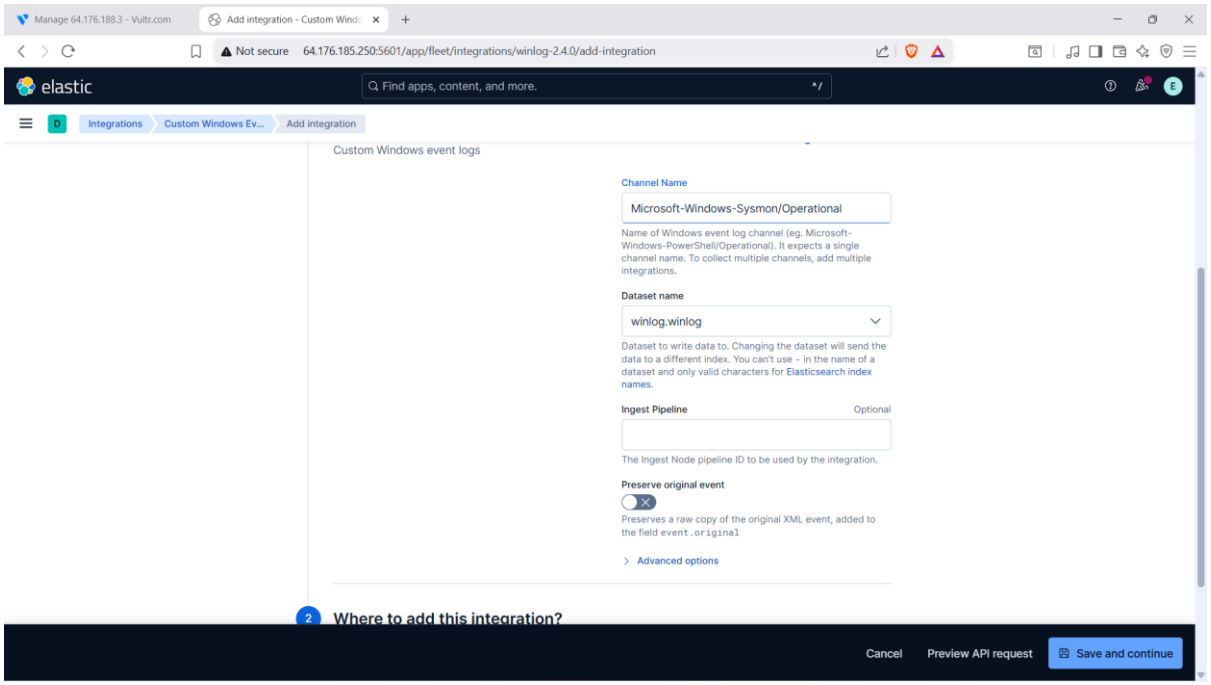


Open the **Event viewer**, head to **application and services logs**, click on **Microsoft**, then to **windows** and then **sysmon**.

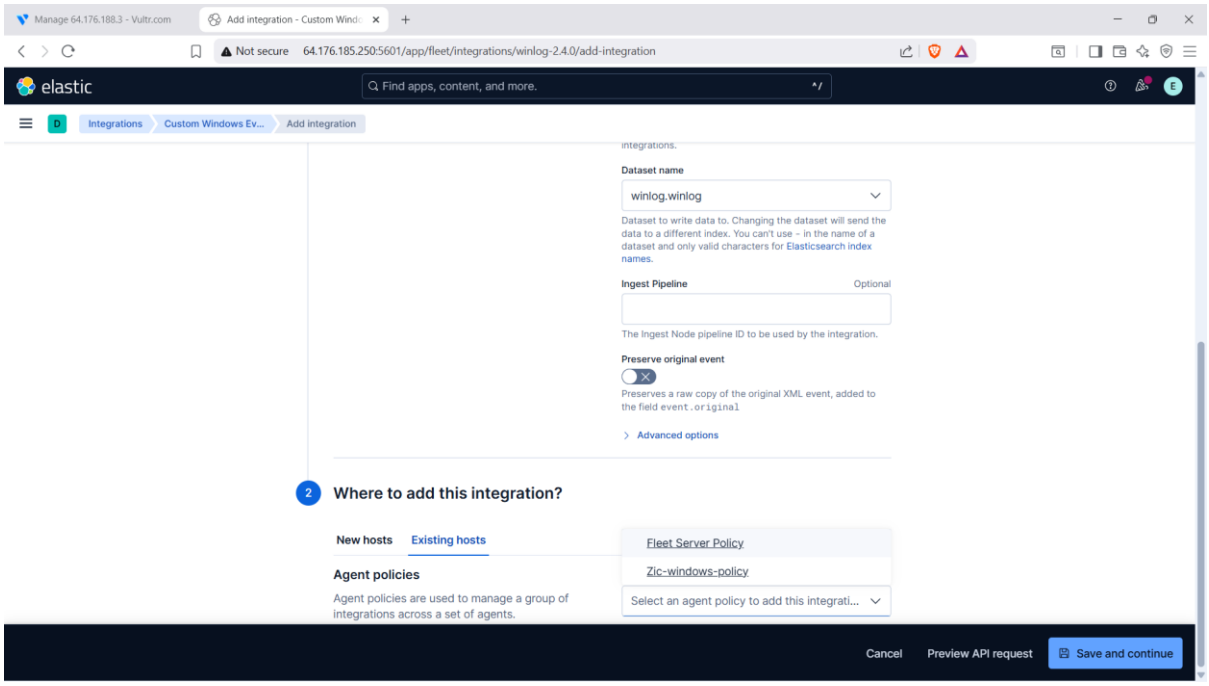


Under **sysmon,** you will see **operational,** right click it and go to **properties**, there is where you will see the full name which is the channel name. Copy the full name and paste in your **channel name.**

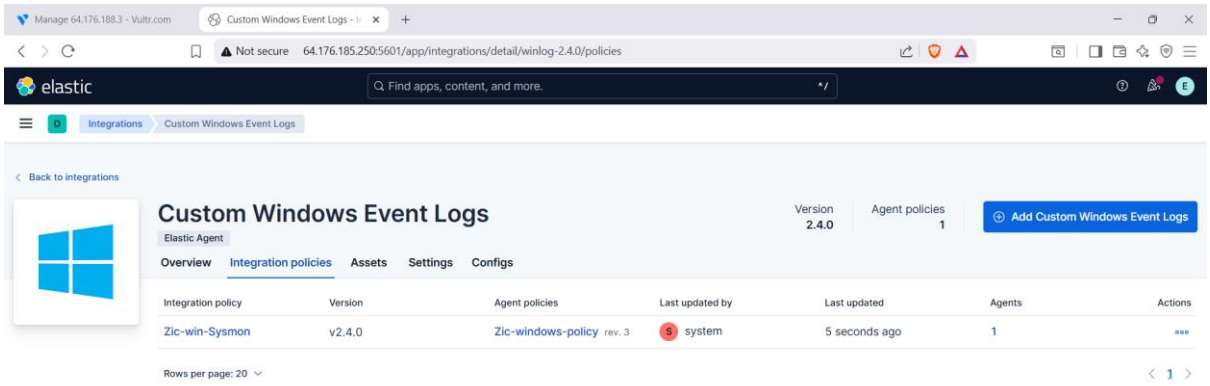




Ensure you add the existing host to an agent policy which is **Zic-windows-policy**.



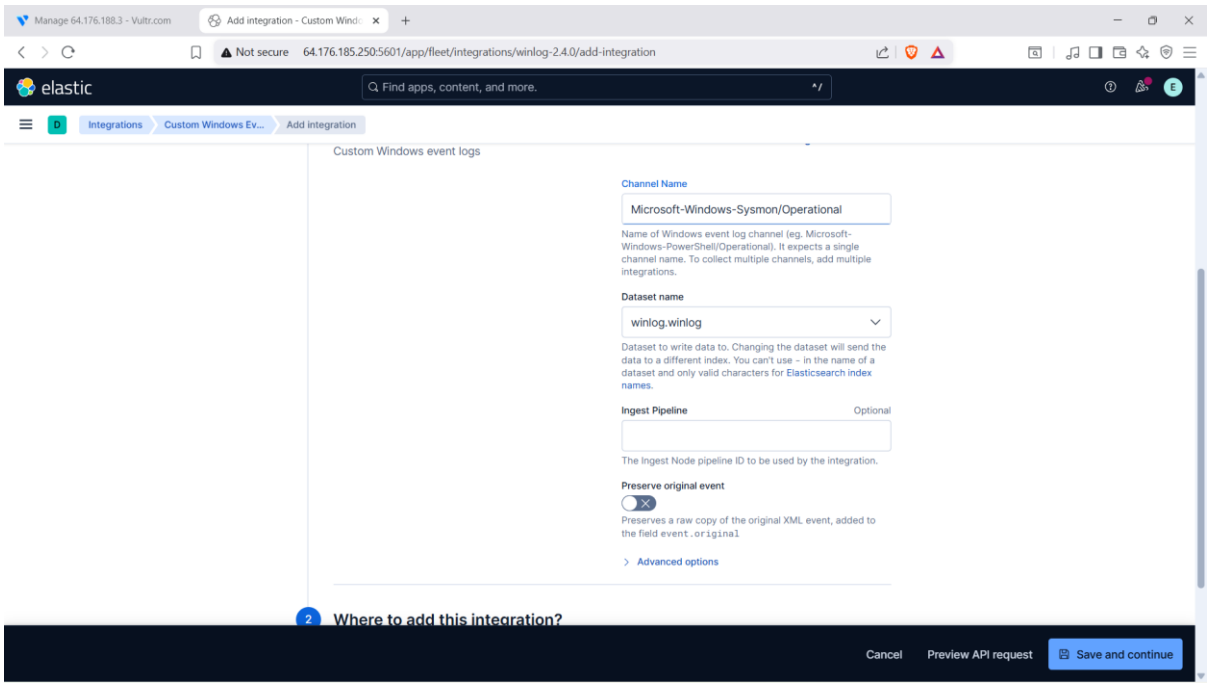
Click on save and continue, then save and deploy. In the screenshot below, it has been integrated.



We successfully integrated Sysmon to the elasticsearch.

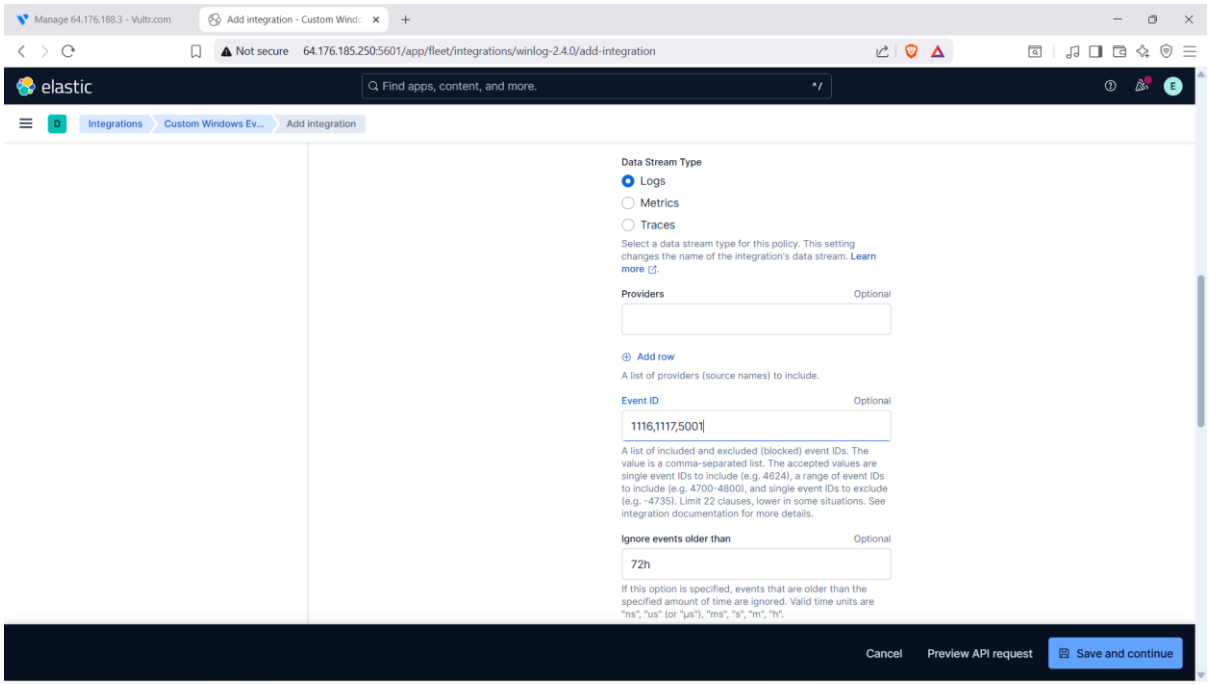
To add windows defender to the elastic search, we carry out the same process as that of sysmon.

Add the **integration name** and **description**, for the **channel name**, instead of **sysmon**, you go to **windows defender**, then **operational**. Right click and copy the **full name** which is the **channel name**.

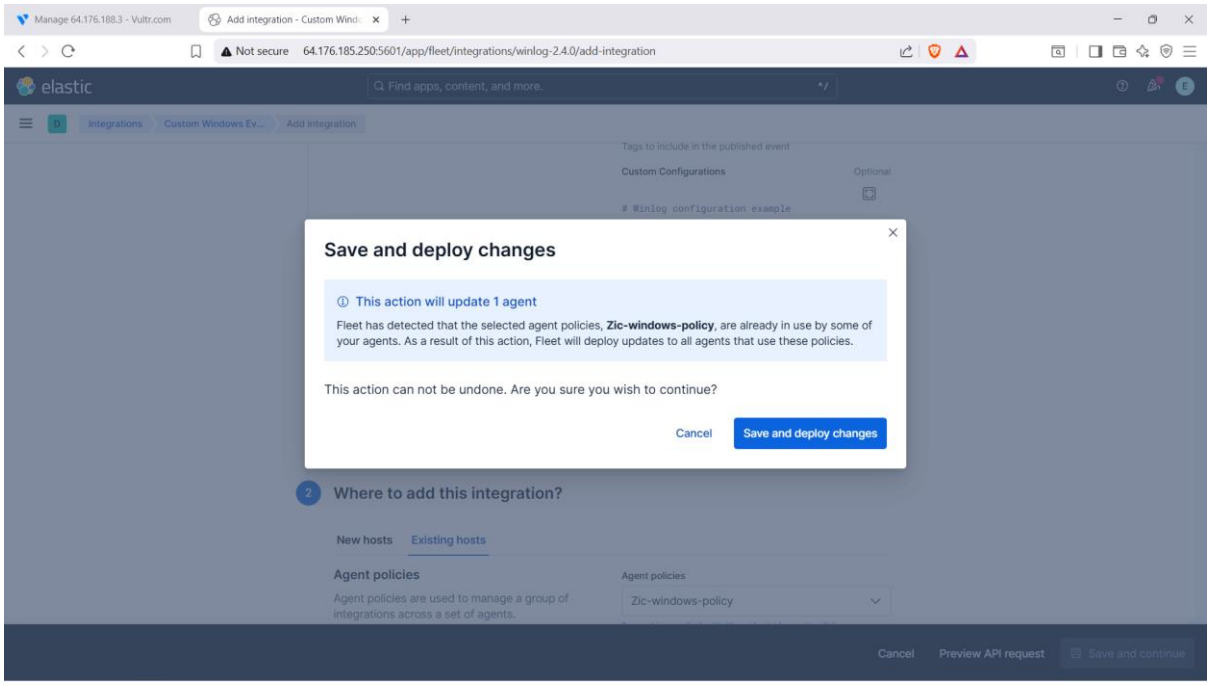


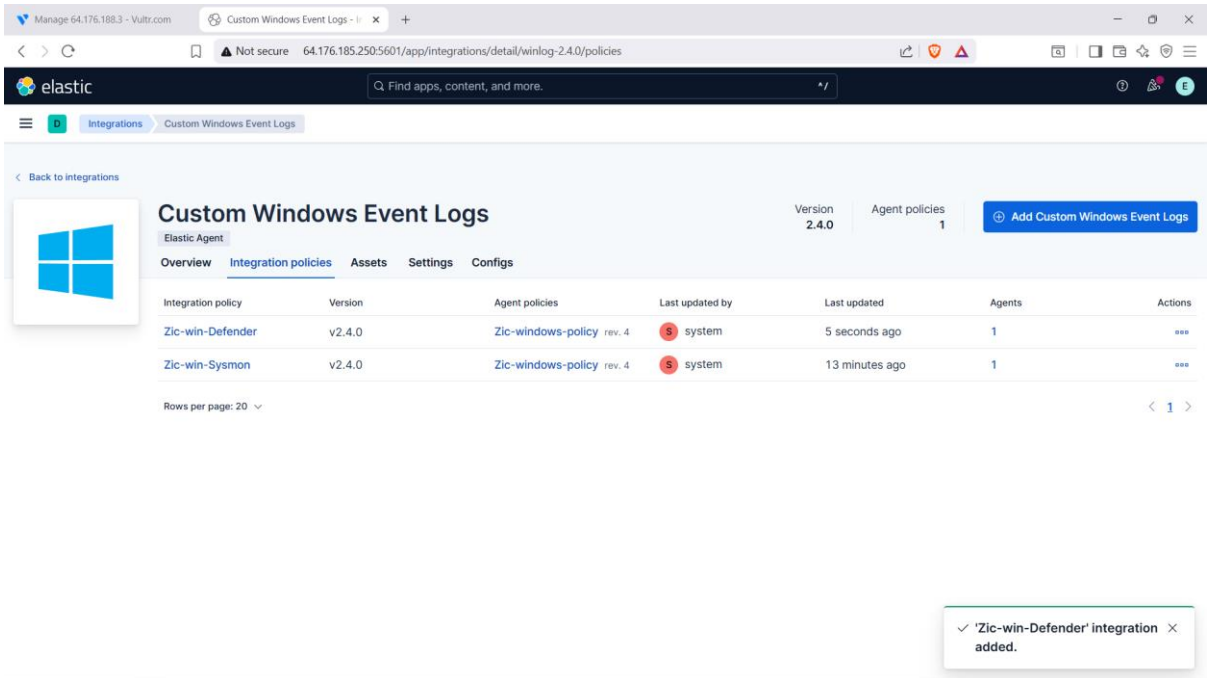
For this, we are not ingesting every log, so we will work with event IDs 1116 (detects malware and other unwanted software), 1117 (performs an action to protect your system from malware) and 5001 (real-time protection is disabled).

You click **advanced options**, you add the event IDs 1116,1117,5001, scroll down to **existing hosts** and select **Zic-windows-policy** for the **agent policy.**



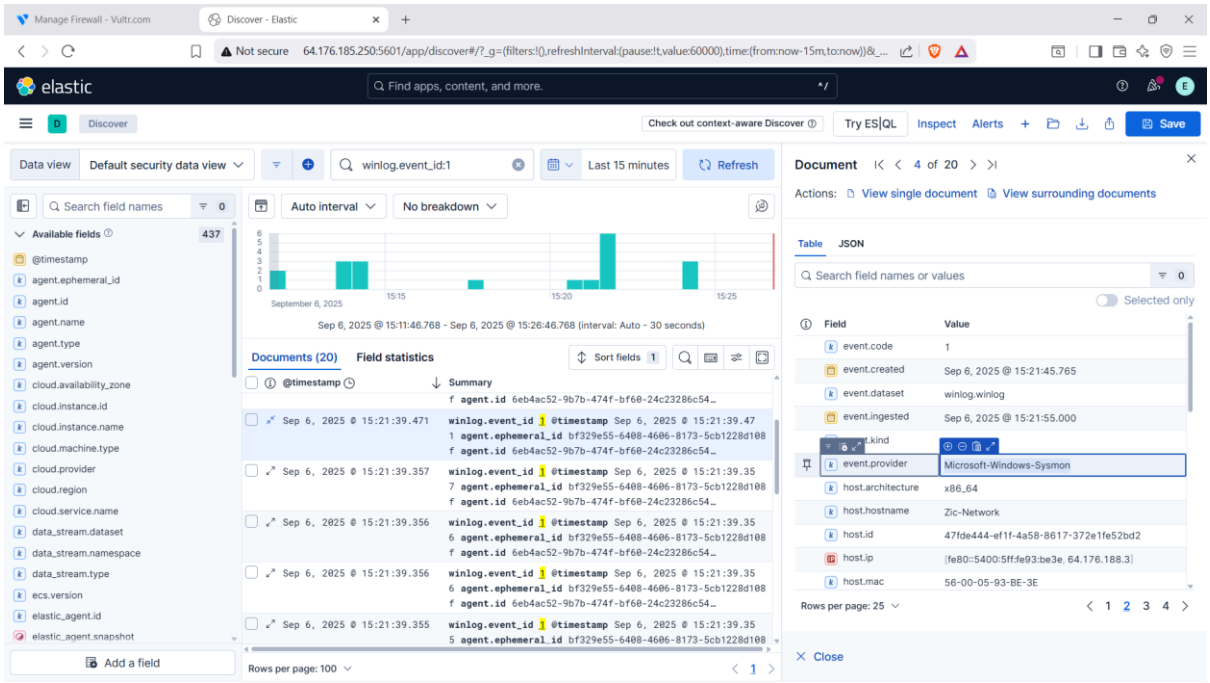
Save and continue,then save and deploy changes.





From the buttom right, you can see the notification **Zic-win-Defender Integration added**. Which shows the Zic-win-Defender has been successfully added to the elasticsearch.

To check if the event IDs we inputted appears in the log.



From the screenshot above, we can see that the event ID 1 appears. Expand it to get more details such as event provider, event code and hostname.

Use of sysmon.

- Tracking process creation (Event ID 1).
- Monitoring network connections (Event ID 3).
- Logging image loads and DLL activity (Event ID 7).
- Providing valuable forensic and threat-hunting data to detect malicious behavior.
- Feeding structured, detailed telemetry into SIEMs like Elasticsearch for real-time analysis.

One challenge I faced was on my windows server. The Microsoft edge browser was giving me error when searching for sysmon, so I had to install google chrome browser and set it up before I could download the sysmon file.