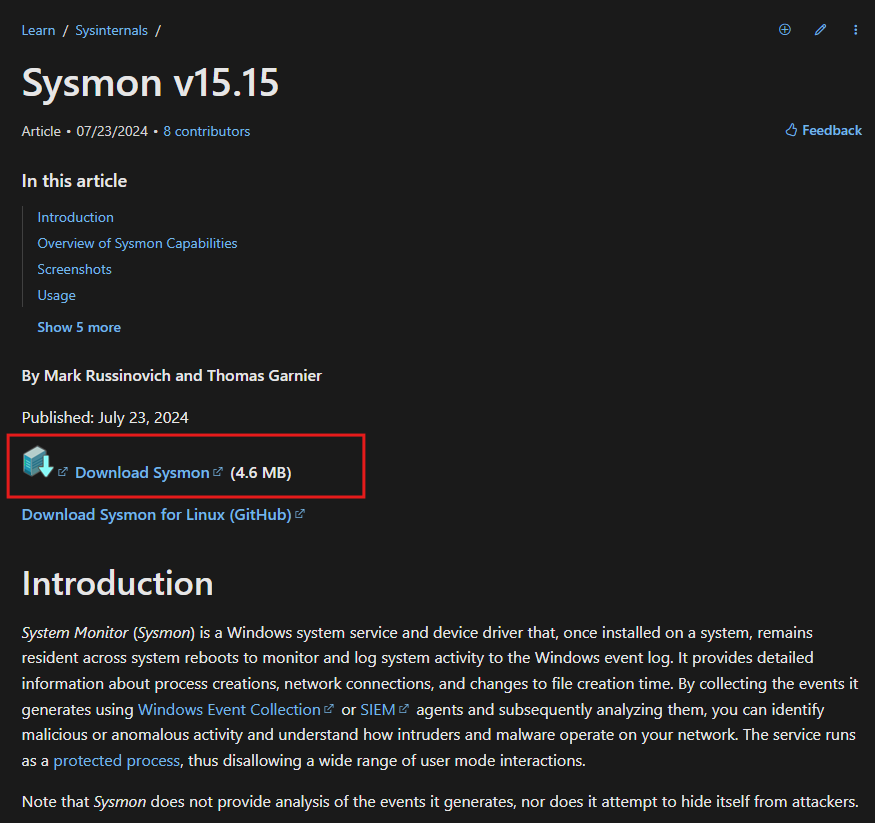
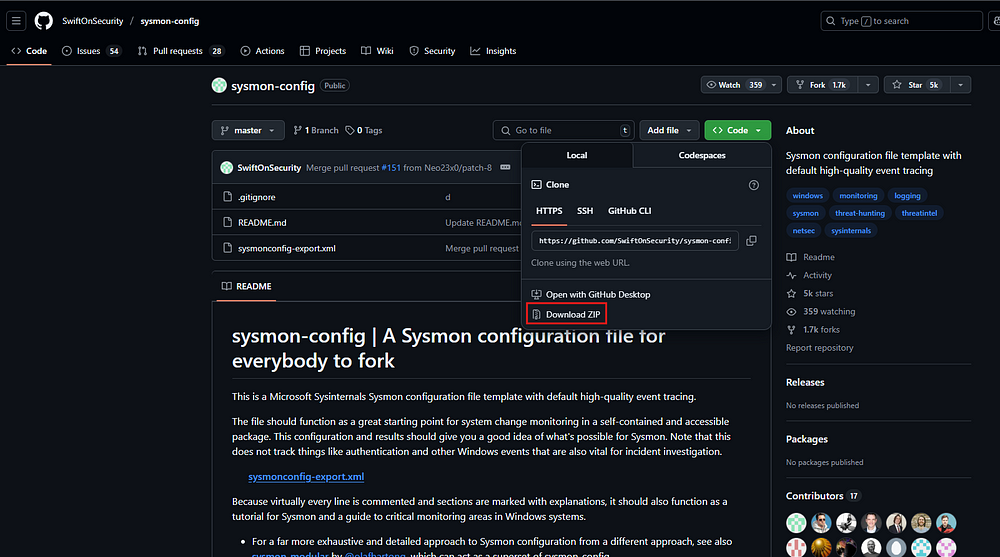
### **Sysmon configuration and setup with Elastic**

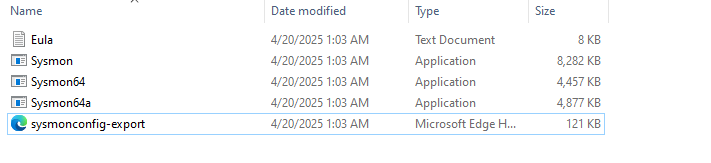
Sysmon, a Windows system service, facilitates the monitoring and logging of system activity to the Windows event log. The implementation of Sysmon, coupled with the ingestion of logs into Elastic, enhances the observability of system events and processes. The Sysmon package can be downloaded from the provided link: [here](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).



Subsequently, deploy the Sysmon configuration file, which is available at the following location:<https://github.com/SwiftOnSecurity/sysmon-config>.



Upon completion of the download, locate the directory containing the downloaded files and extract the contents of the zip archives. Subsequently, transfer the configuration XML file to the Sysmon directory.

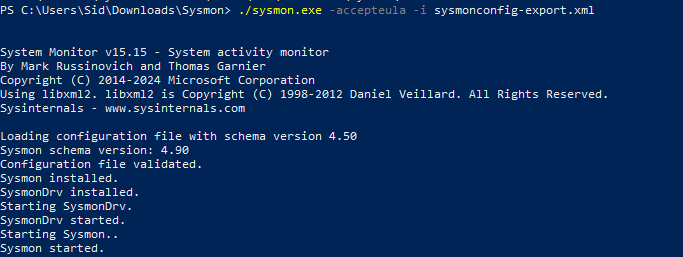


Subsequently, initiate an elevated PowerShell session and proceed to the aforementioned directory.

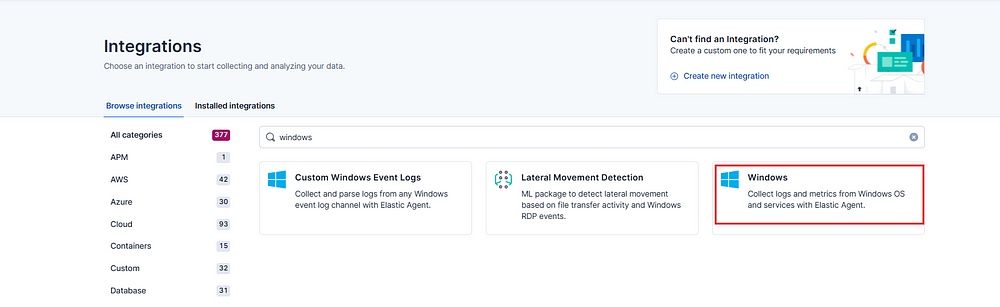


Execute the subsequent command:

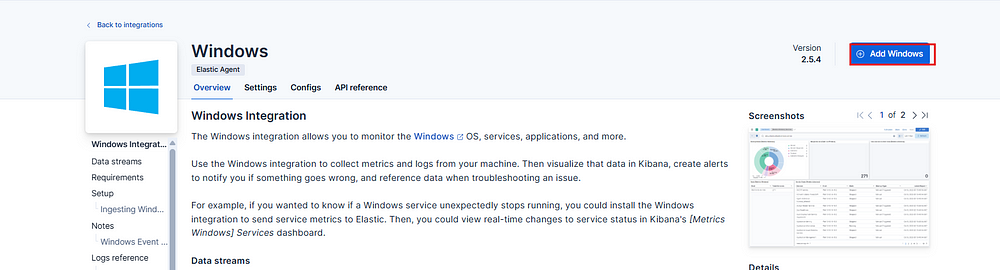
./sysmon.exe -accepteula -i sysmonconfig-export.xml



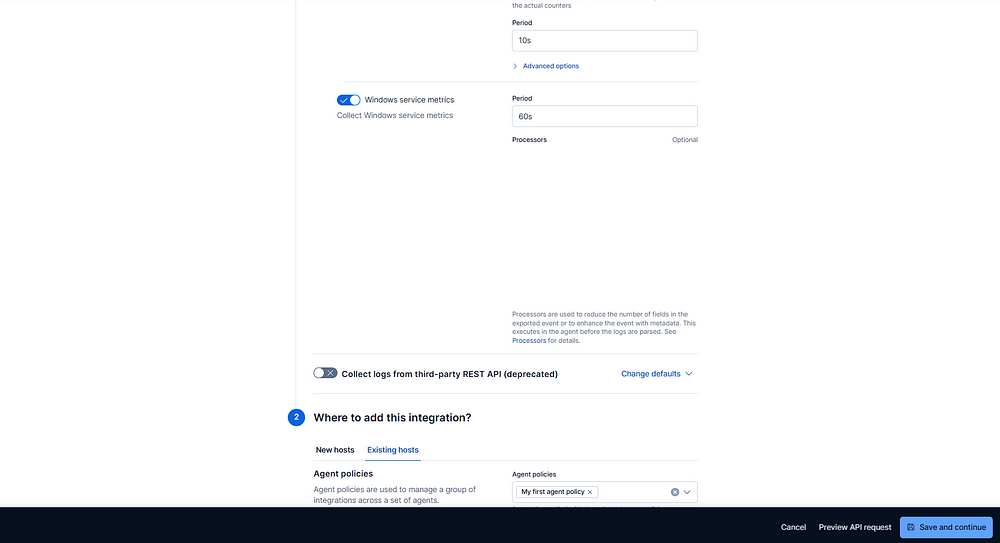
System Monitor (Sysmon) has been successfully installed. Configuration of Elastic to receive logs from Sysmon is required. Navigate to Integrations and search for Windows on the Elastic Cloud platform.



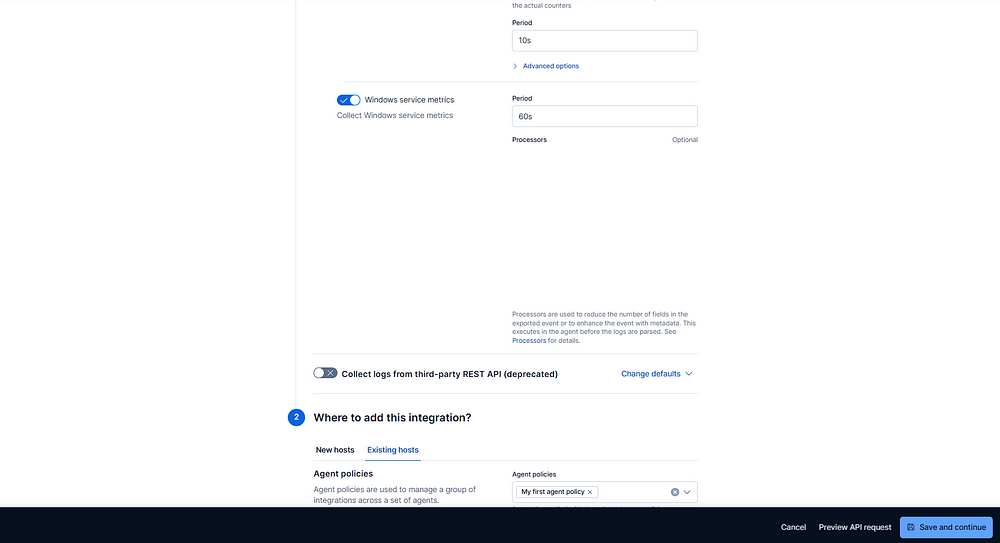
Subsequently, select the "Windows integration" option as depicted above.



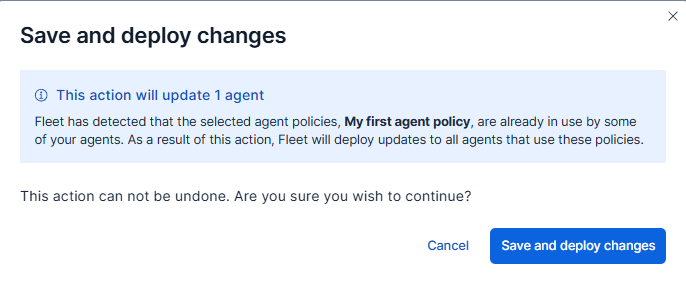
Then click on Add Windows.



Subsequently, within the section designated "Where to add this integration?", opt for "Existing hosts" and subsequently choose "My first agent policy". Refer to the Elastic configuration blog for comprehensive instructions on establishing the Elastic agent setup.

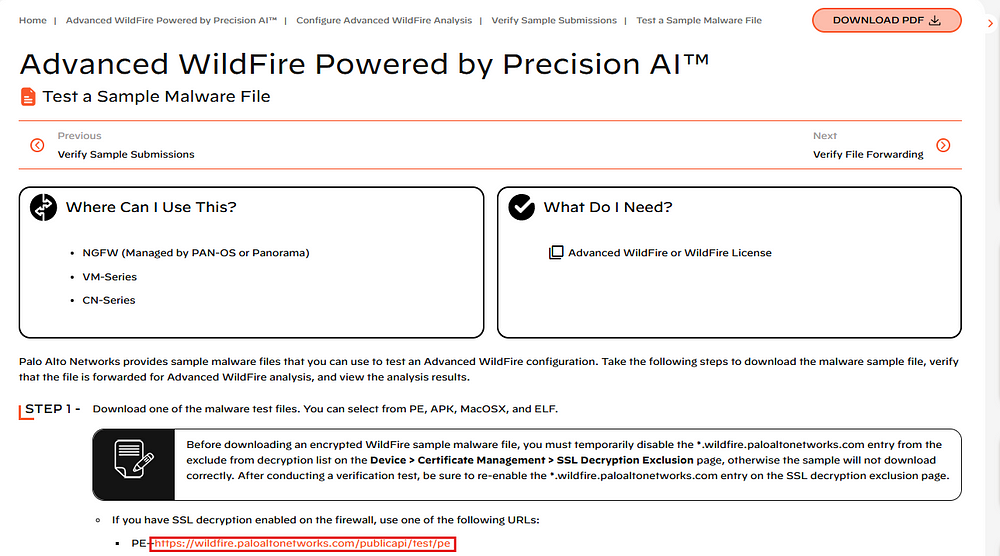


Subsequently, select "Save and continue," followed by "Save and deploy changes."



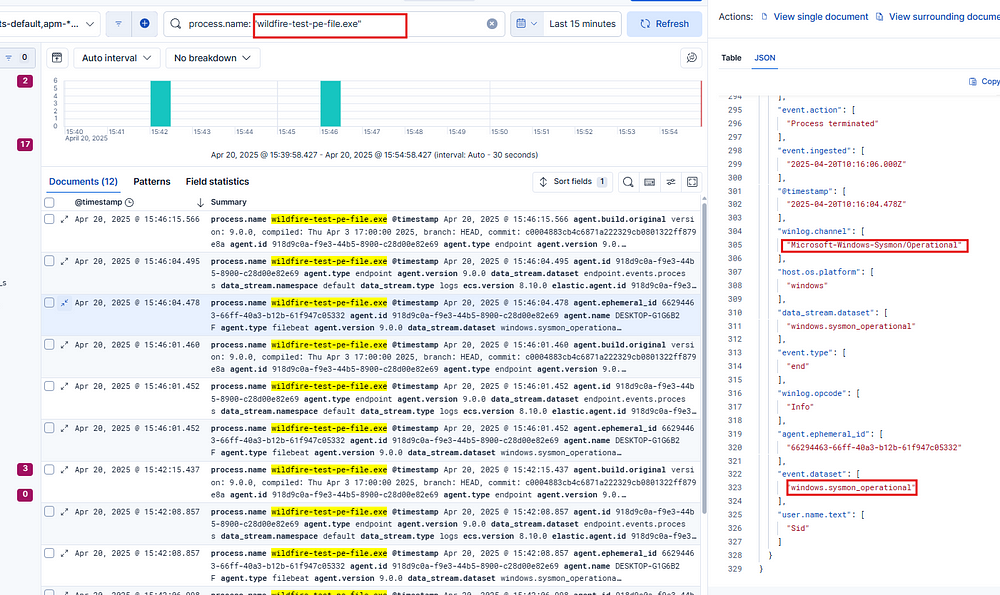
To verify the operational status of the Sysmon integration, a malware sample will be procured and executed to observe the resulting log generation. The malware can be obtained from the provided link: [here](https://docs.paloaltonetworks.com/advanced-wildfire/administration/configure-advanced-wildfire-analysis/verify-wildfire-submissions/test-a-sample-malware-file).

It is imperative that this procedure be conducted exclusively within an isolated environment.



Execute the downloaded file exclusively within an isolated environment.





It is evident from the aforementioned data that Sysmon logs are being successfully ingested into the Elastic Cloud environment.