Detection Engineering in a Homelab — Part 3: Setting Up Sysmon for Enhanced Telemetry

F Frederick Adigun 4 min read · Aug 20, 2025

By default, Wazuh collects a lot of logs from the Windows Event Viewer, but it is not exhaustive. Many potentially useful events, even in the Microsoft Windows Applications directory, are not tracked.

To boost our telemetry, we can use **Sysmon**, a free Microsoft tool from the Sysinternals suite. Sysmon provides detailed logging that greatly improves your chances of detecting malicious activity. It can monitor many types of events and is highly customizable. Although a configuration file is optional, it is recommended to tailor it to your environment. The config file, usually in XML, specifies which events to log and which to ignore. There are many ready-made Sysmon configs available online. For this setup, I will use the configuration file created by Olaf. This Sysmon installation will be performed on the Windows VM that has the Wazuh agent installed.

First, navigate here to download download Sysmon. Download the Sysmon executable file for windows (Fig. 1).

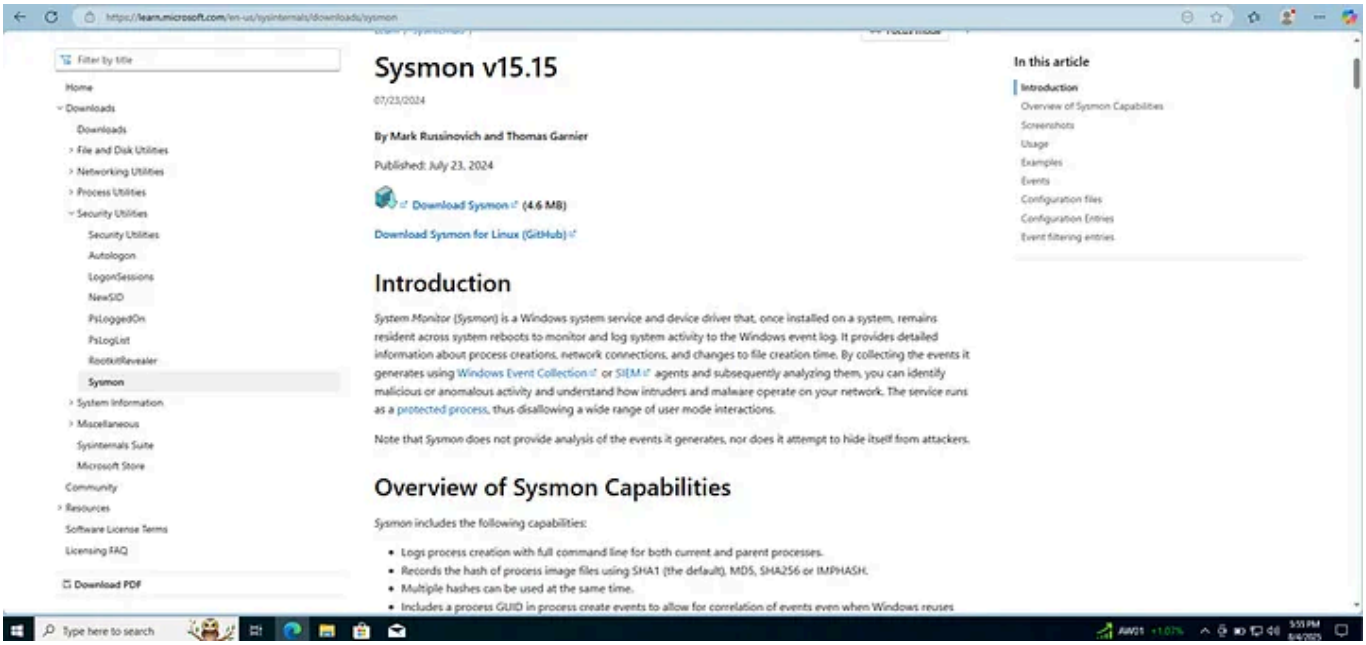

Fig. 1

Also download the configuration file by Olaf from the github page.

On the GitHub page, click on *sysmonconfig.xml* on the left pane, then click on **Raw**, then right-click and choose **Save As** to save the file, for example as `sysmonconfig.xml` (Fig. 2, 3, 4).

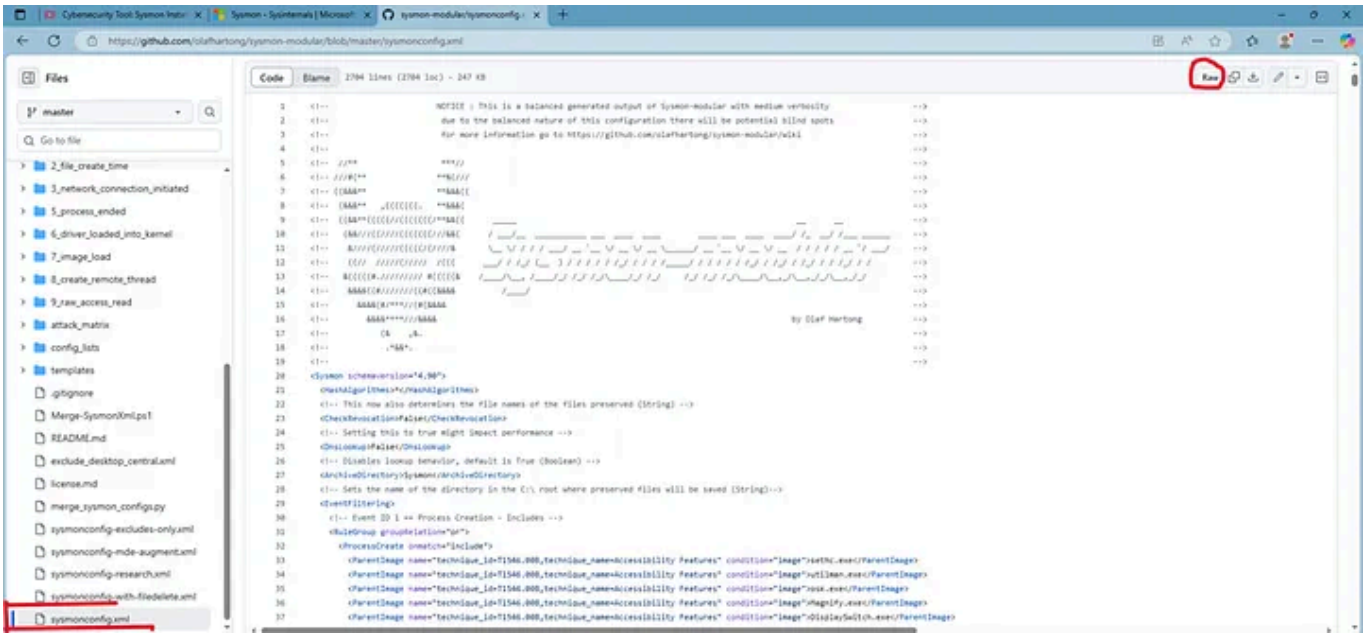

Fig. 2

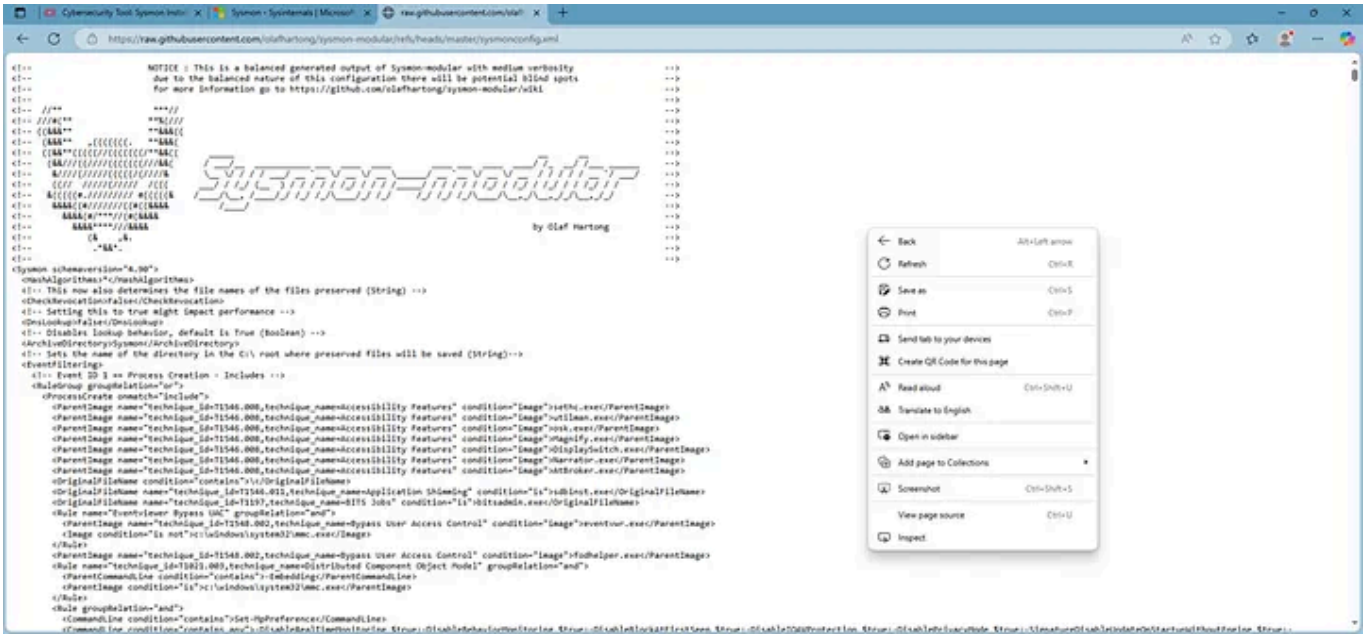

Fig. 3

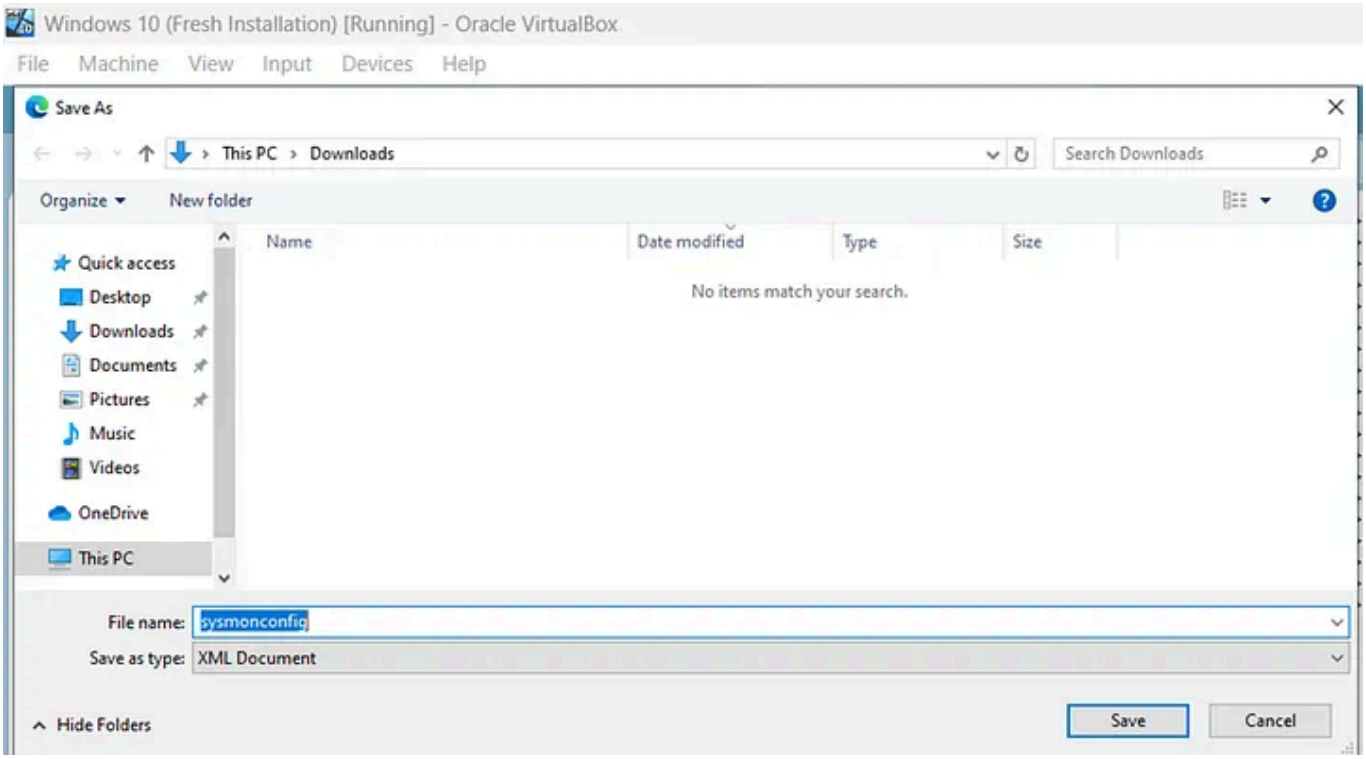

Fig. 4

Once Sysmon is downloaded, extract the contents (Fig. 5).

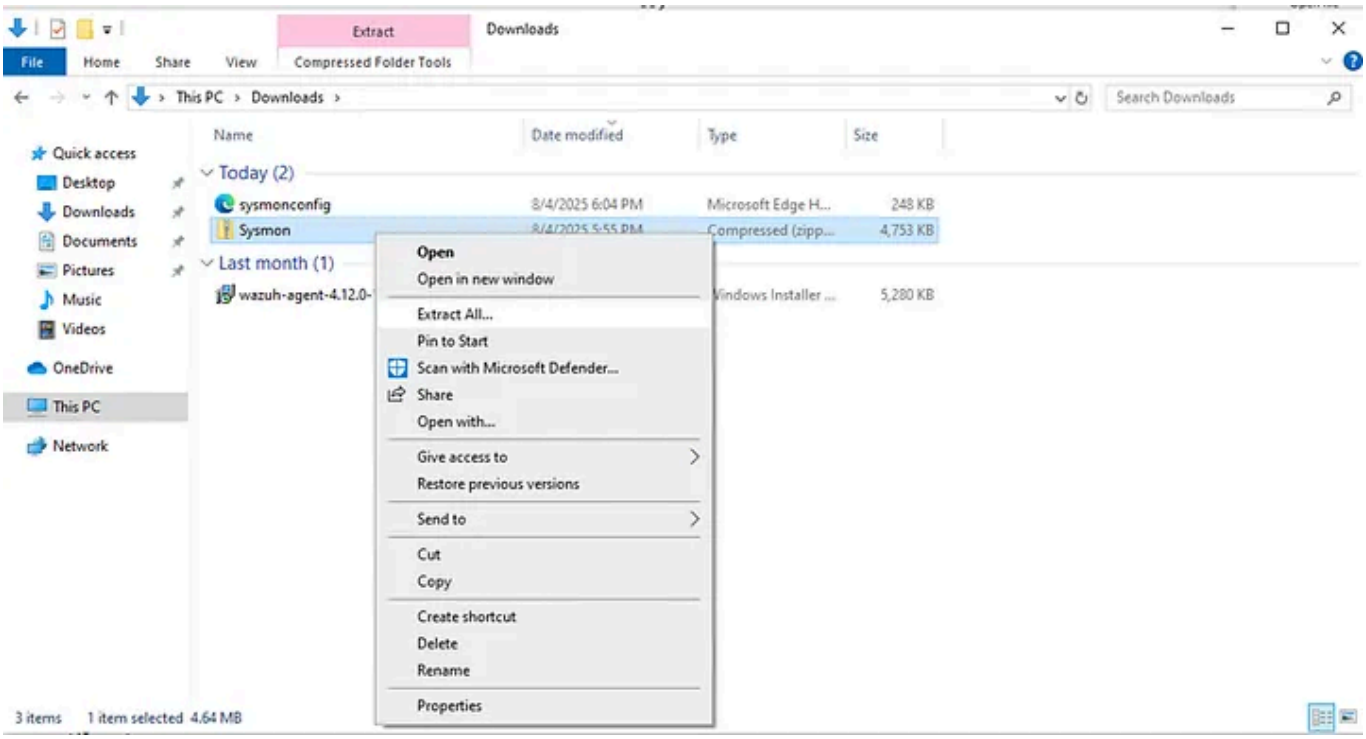

Fig. 5

Note: You can use the Sysmon configuration provided by Wazuh instead of the one by Olaf. It is available here.

Next, open PowerShell with administrator privileges and navigate to the extracted folder by using the `cd` command (Fig. 6, 7, 8).

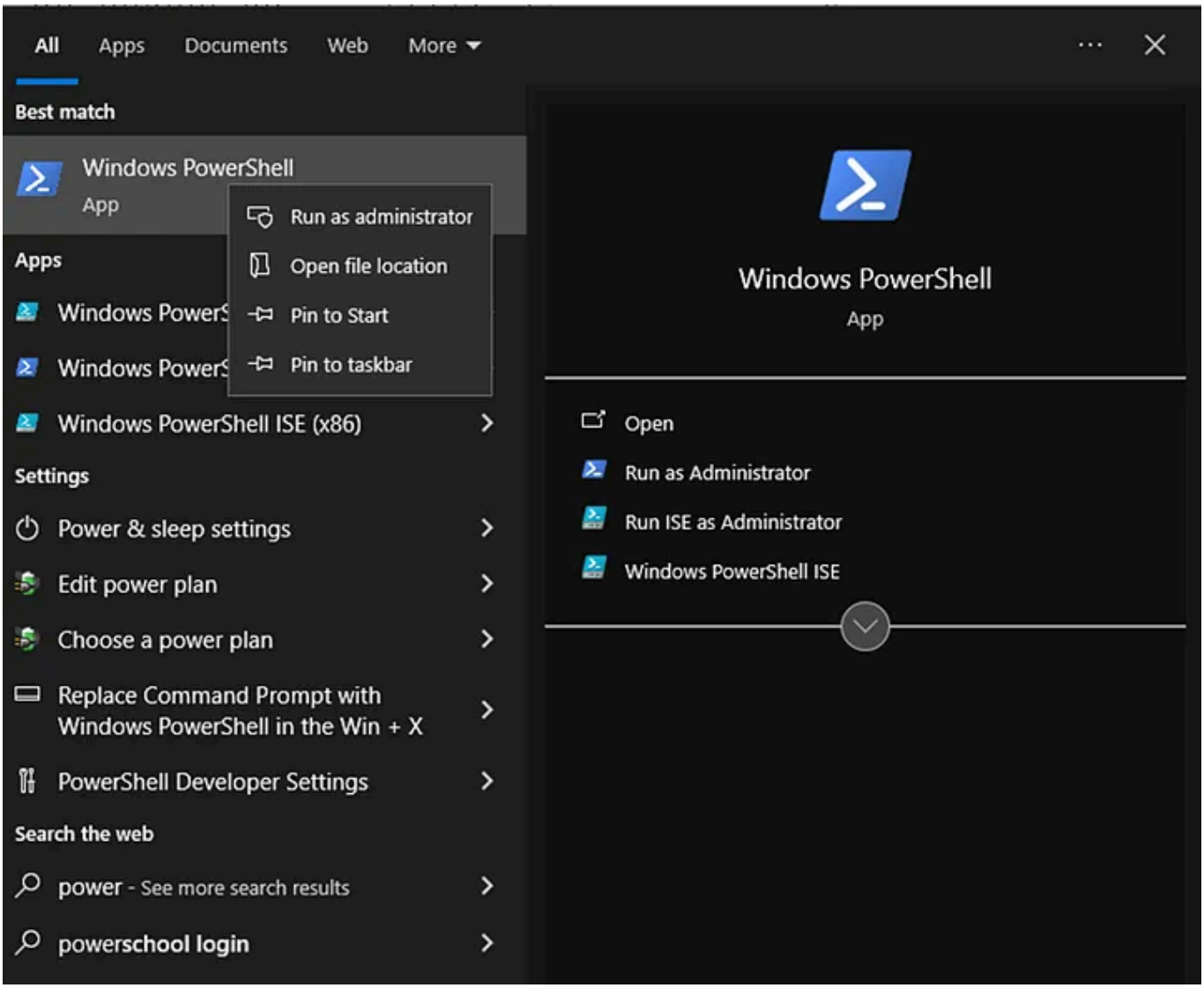

Fig. 6

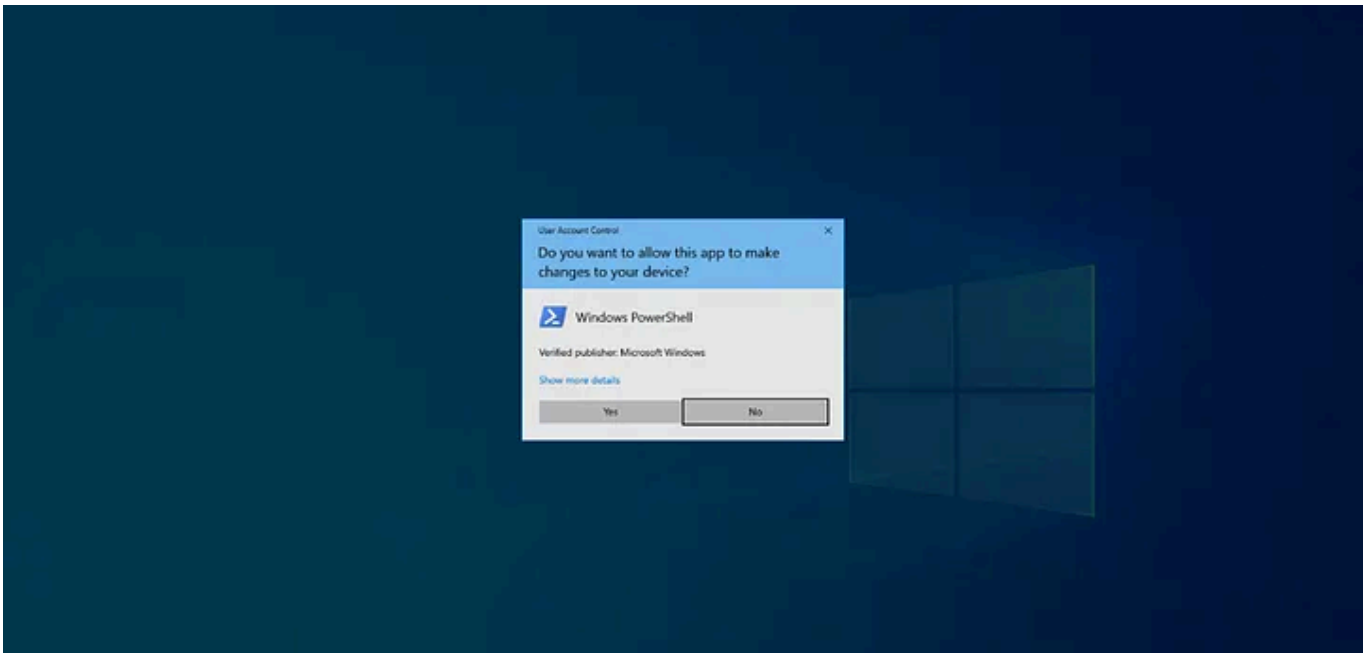
User Account Control
Do you want to allow this app to make changes to your device?
Windows PowerShell
Verified publisher: Microsoft Windows
Show more details
Yes
No

Fig. 7

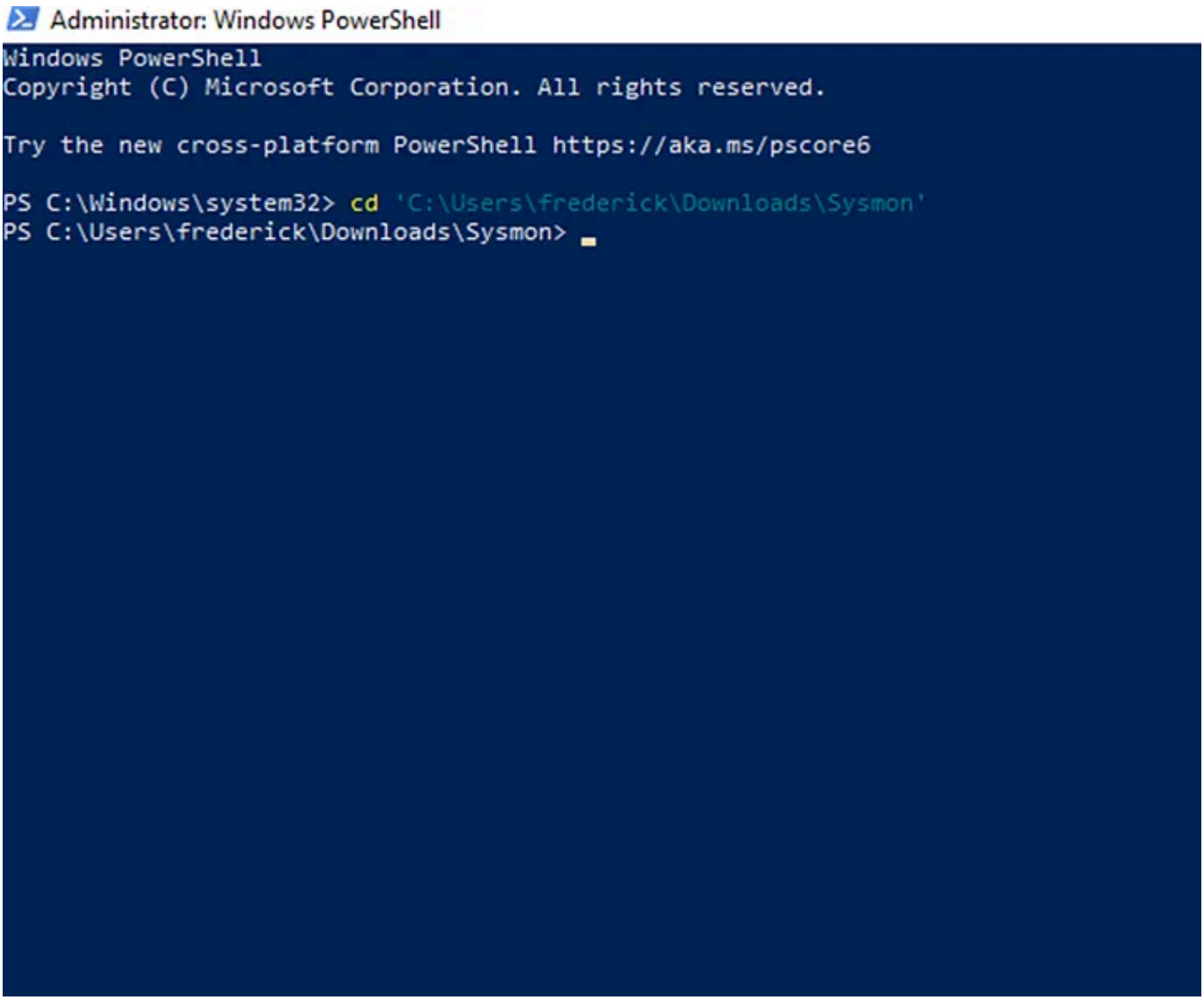
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> cd 'C:\Users\frederick\Downloads\Sysmon'
PS C:\Users\frederick\Downloads\Sysmon>

Fig. 8

Copy the Sysmon config file into the same directory as the extracted folder (Fig. 9).

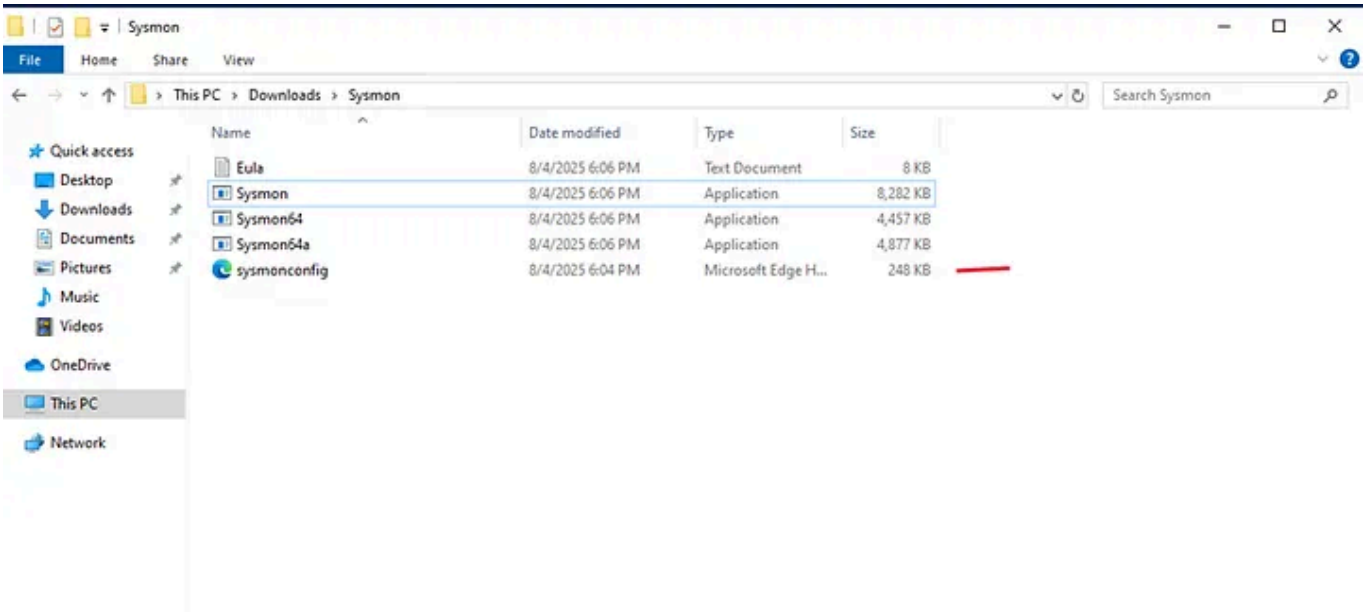

Fig. 9

You'll notice there are several executables; I will use `Sysmon64.exe` for 64-bit systems.

On Powershell session that was started, type `.\Sysmon64.exe`. Pressing enter will display the help menu and information about installation (Fig. 10).

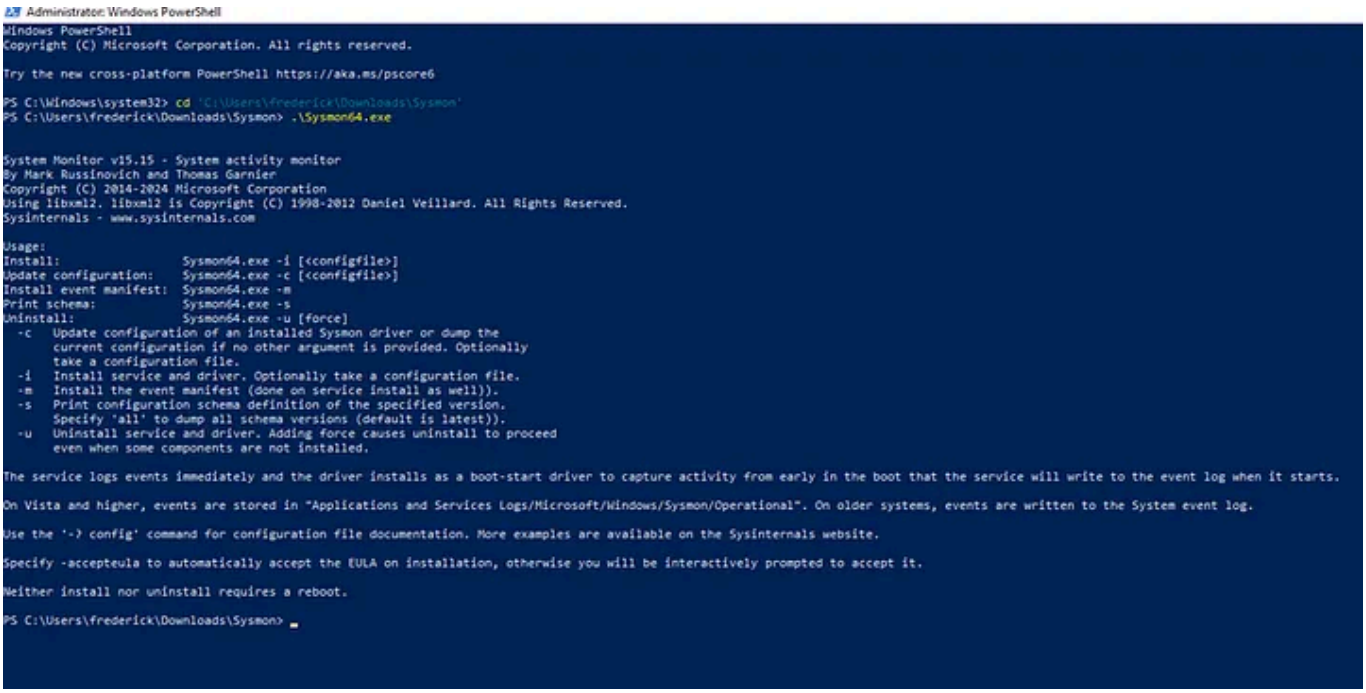

Fig. 10

To install it, type `.\Sysmon64.exe -i .\sysmonconfig.xml` in PowerShell and click enter (Fig. 11). Accept the license agreement and sysmon will be installed (Fig. 12).

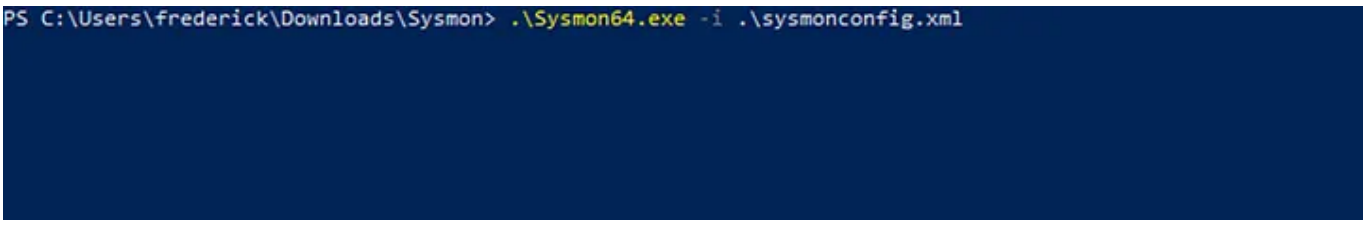

Fig. 11

Fig. 12

To check whether Sysmon installed successfully, go to the Start Menu, search for “Services,” and look for Sysmon in the list, it should there (Fig. 13).

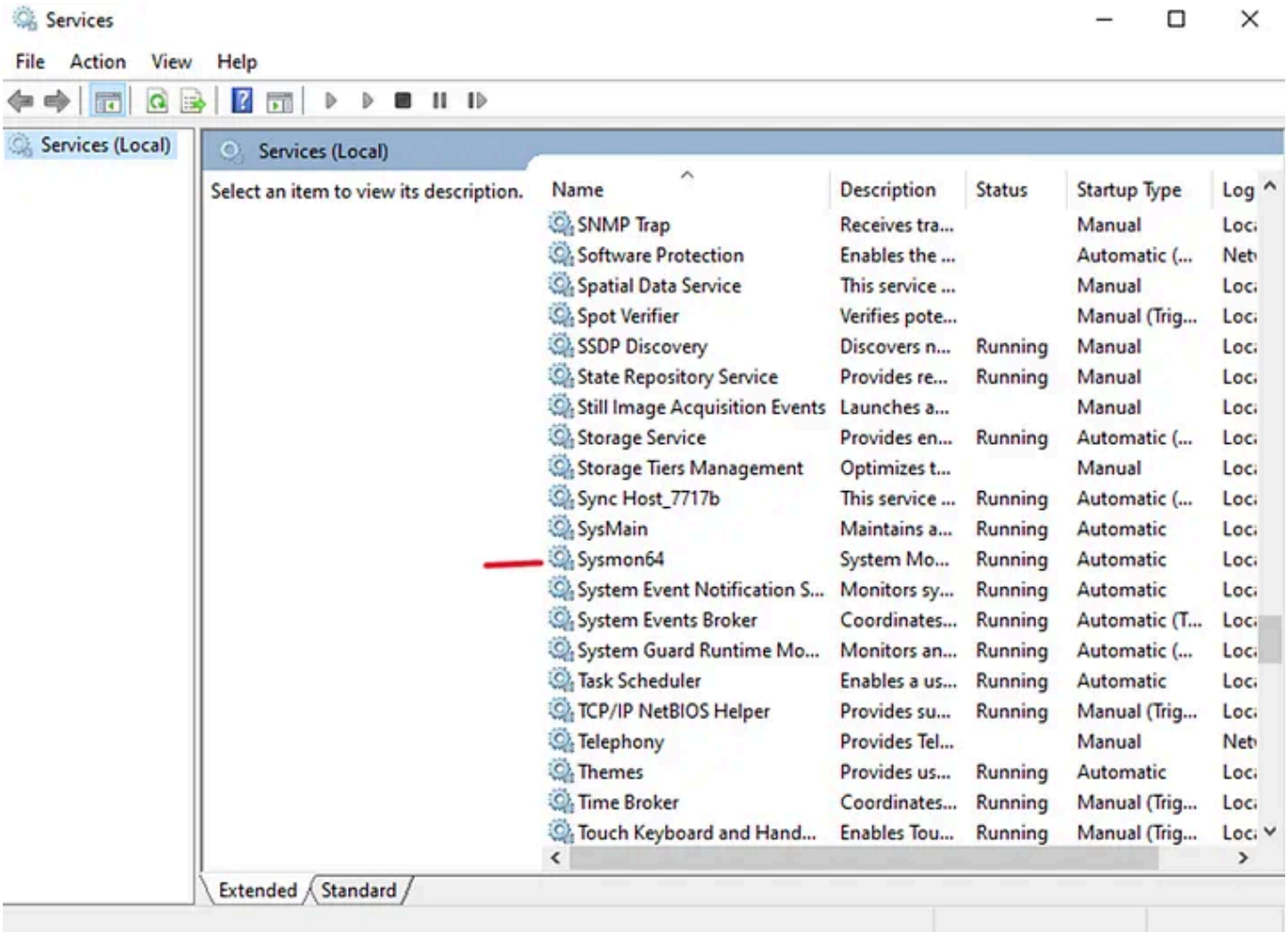

Fig. 13

You can also check the Event Viewer by going to Applications and Services **Logs** > **Microsoft** > **Windows**, and looking for Sysmon. You should find it installed. Expand the Sysmon dropdown, select ‘Operational,’ and view the rich telemetry that can help detect suspicious activity on your system.

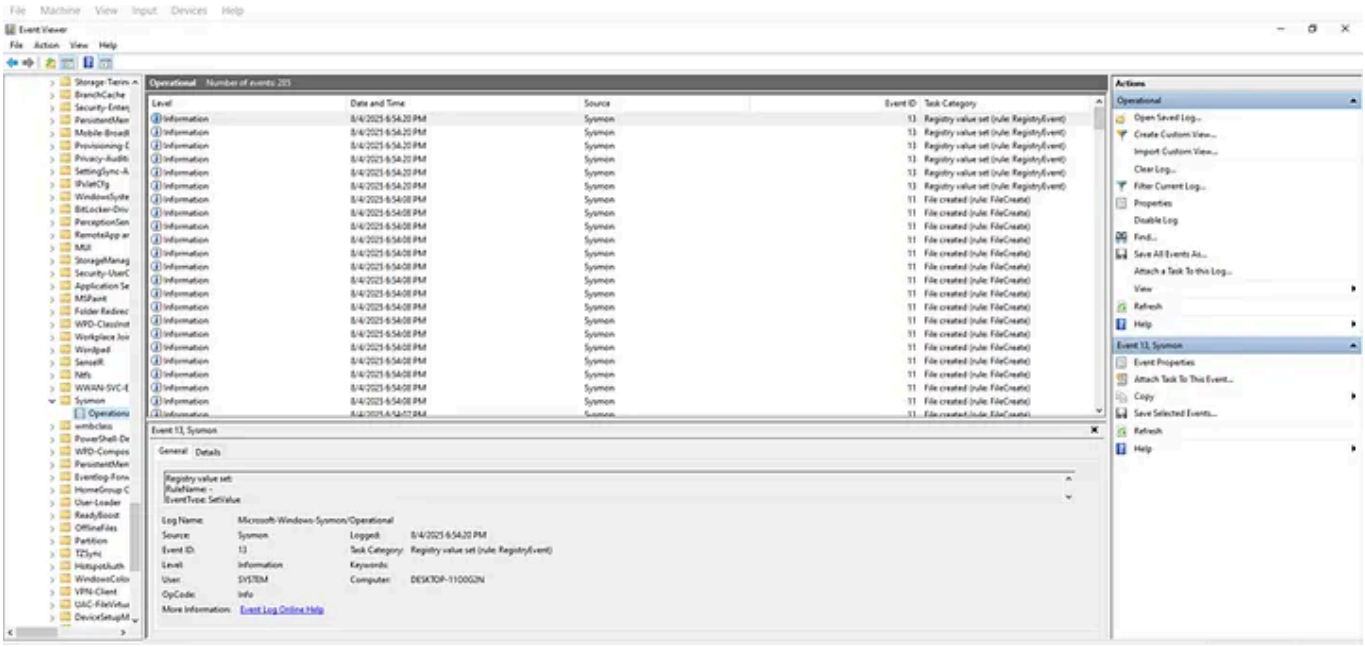

Fig. 14

Building on Parts 1 and 2, we've installed Sysmon to provide deep visibility through telemetry, further enhancing the detection of malicious activity.

Detection Engineering | Sysmon | Wazuh | Homelab | Cybersecurity

F

Written by Frederick Adigun

3 followers · 2 following

Edit profile

No responses yet

F Frederick Adigun