

Open in app ↗

 Search Write 7 F

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

 F

Frederick Adigun · 4 min read · Aug 20, 2025

 15

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 Sysmon. Download the Sysmon executable file for windows (Fig. 1).

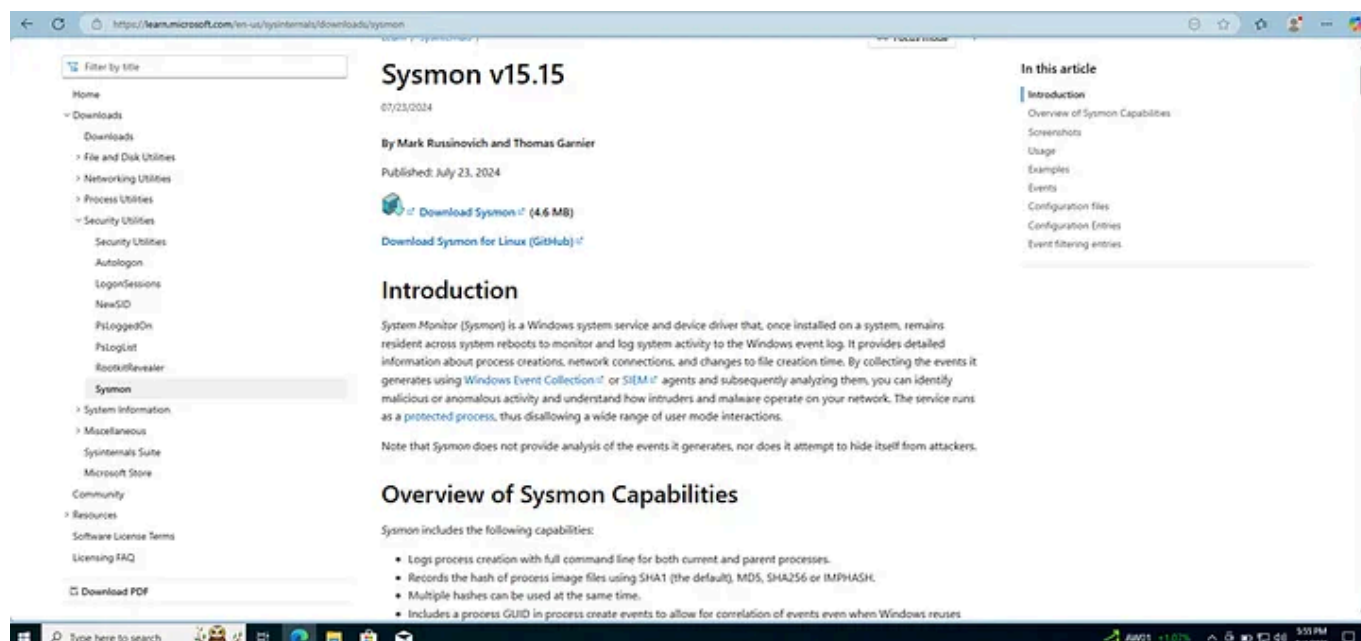


Fig. 1

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).

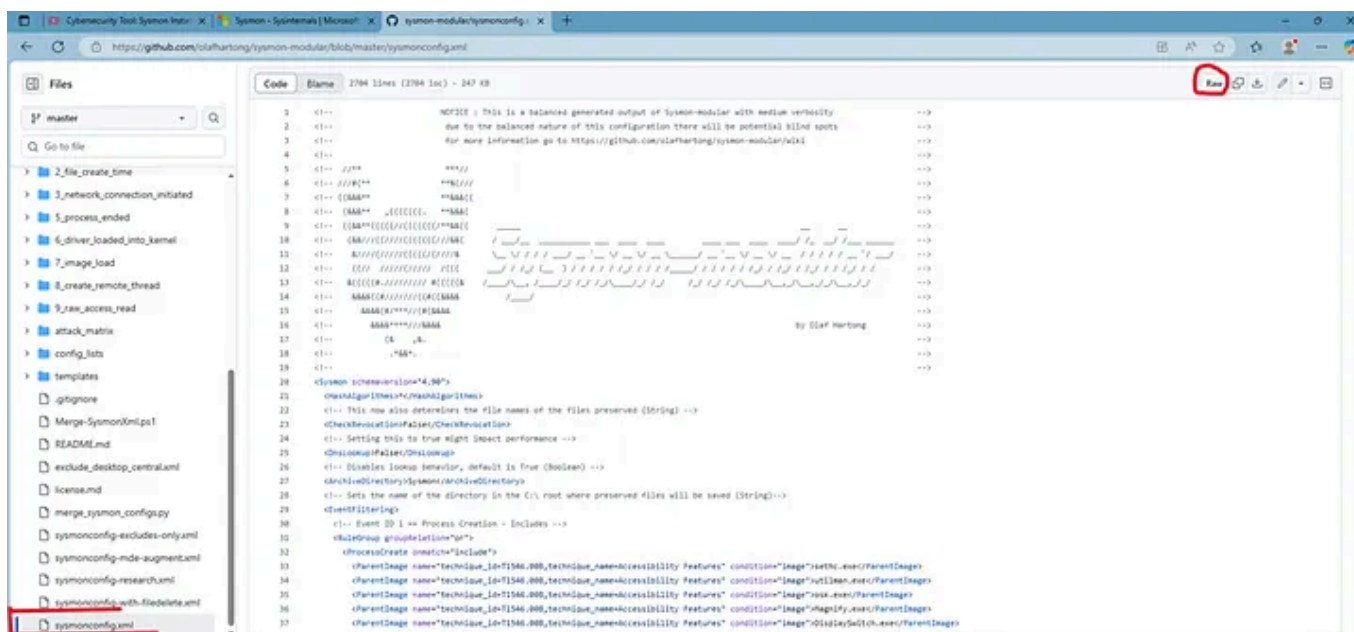


Fig. 2

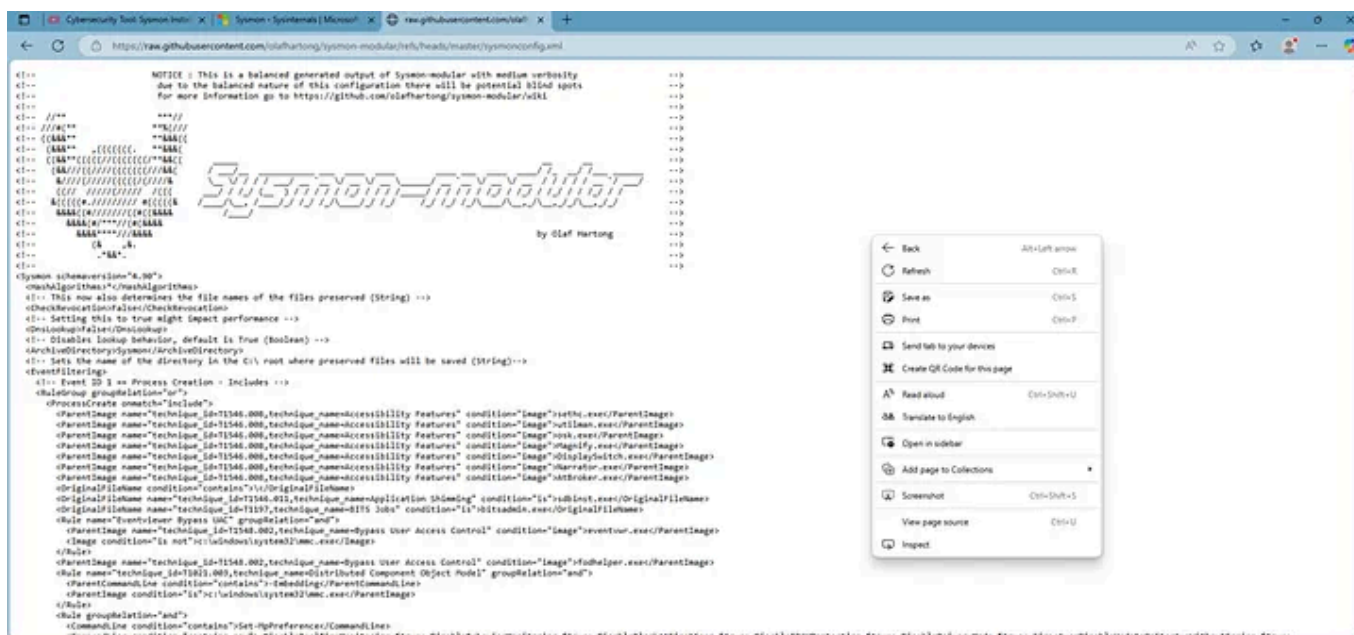


Fig. 3

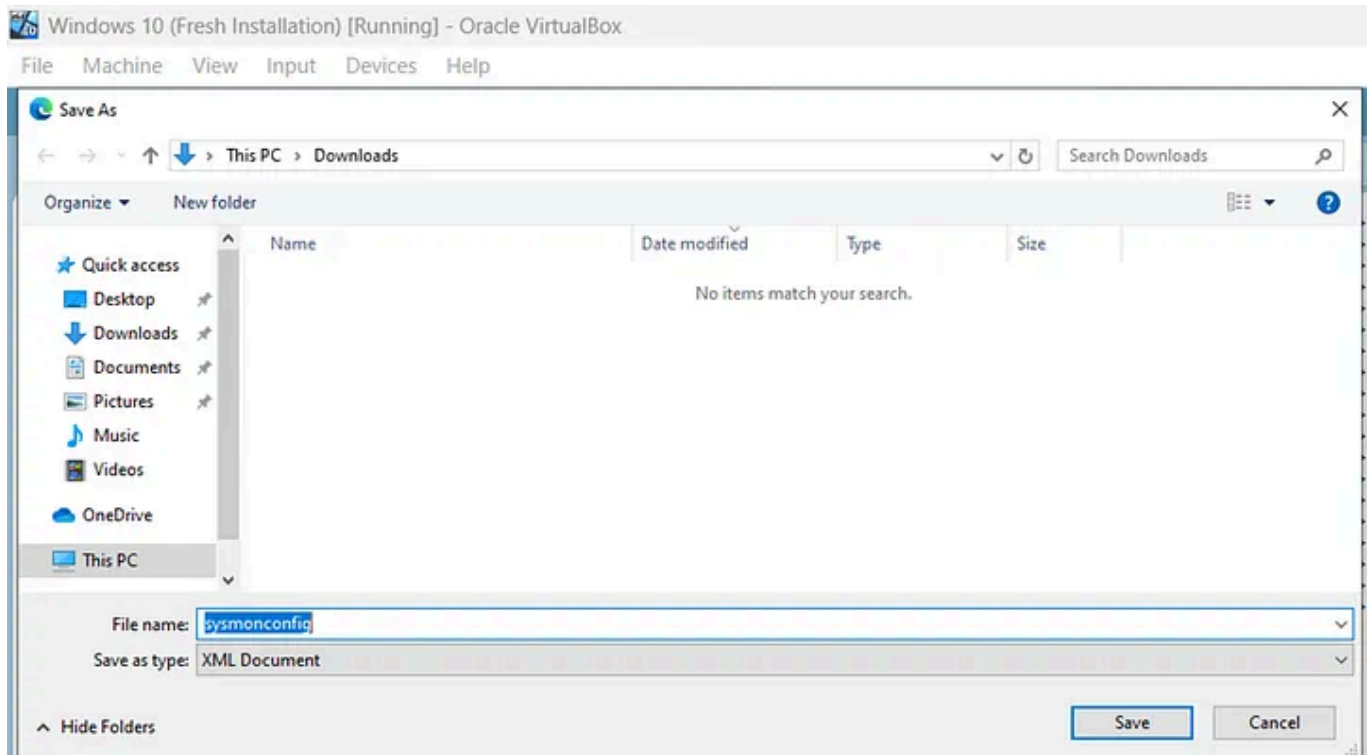


Fig. 4

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

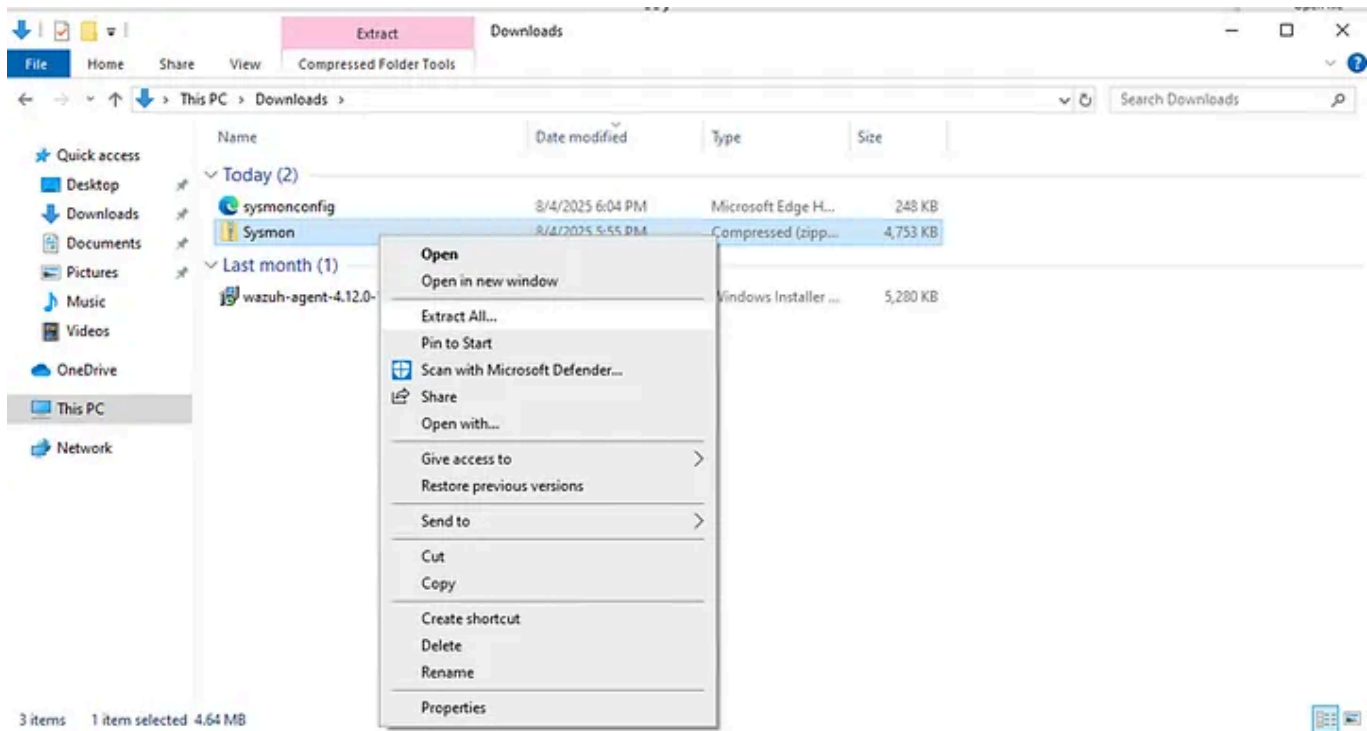


Fig. 5

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).

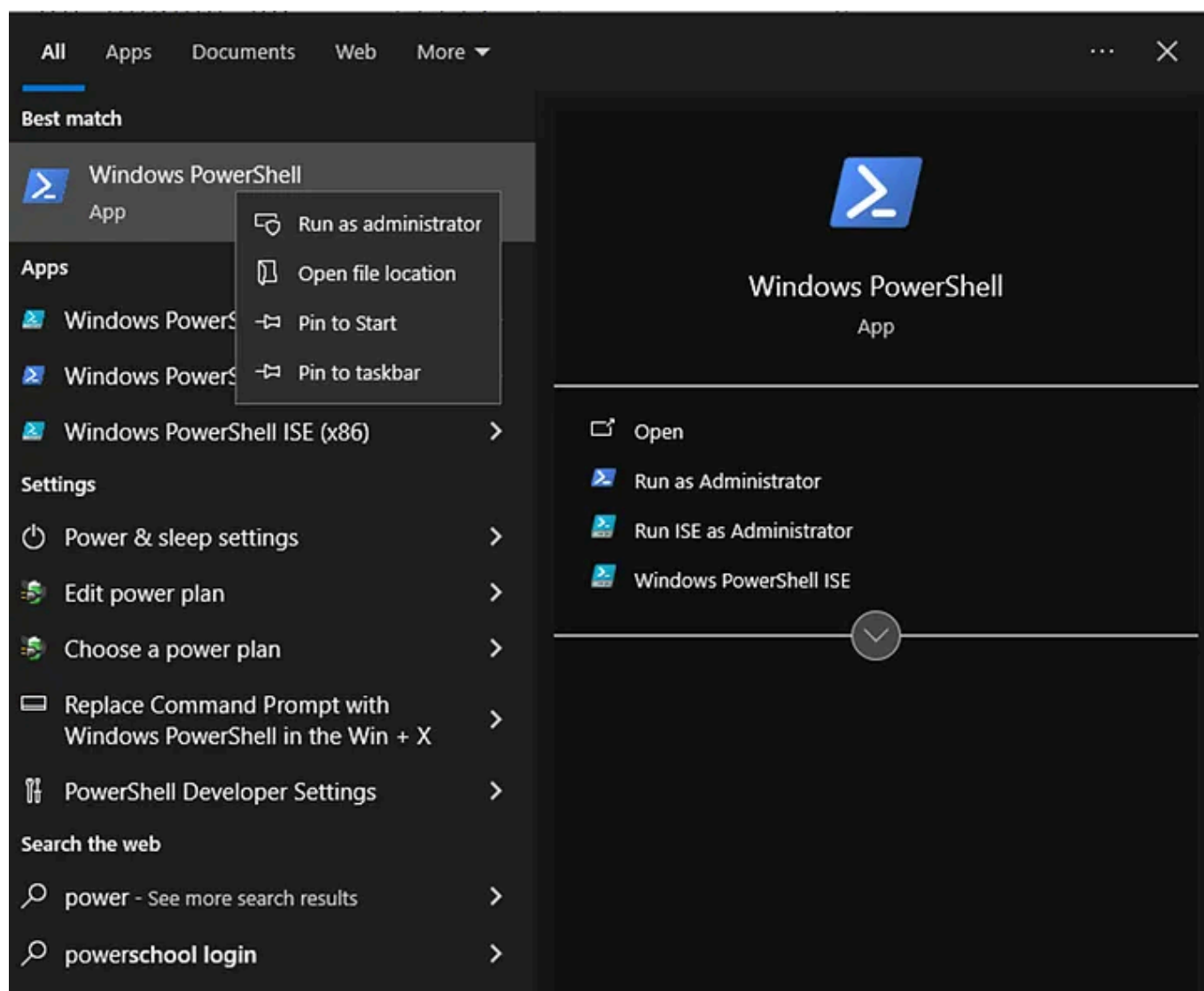


Fig. 6

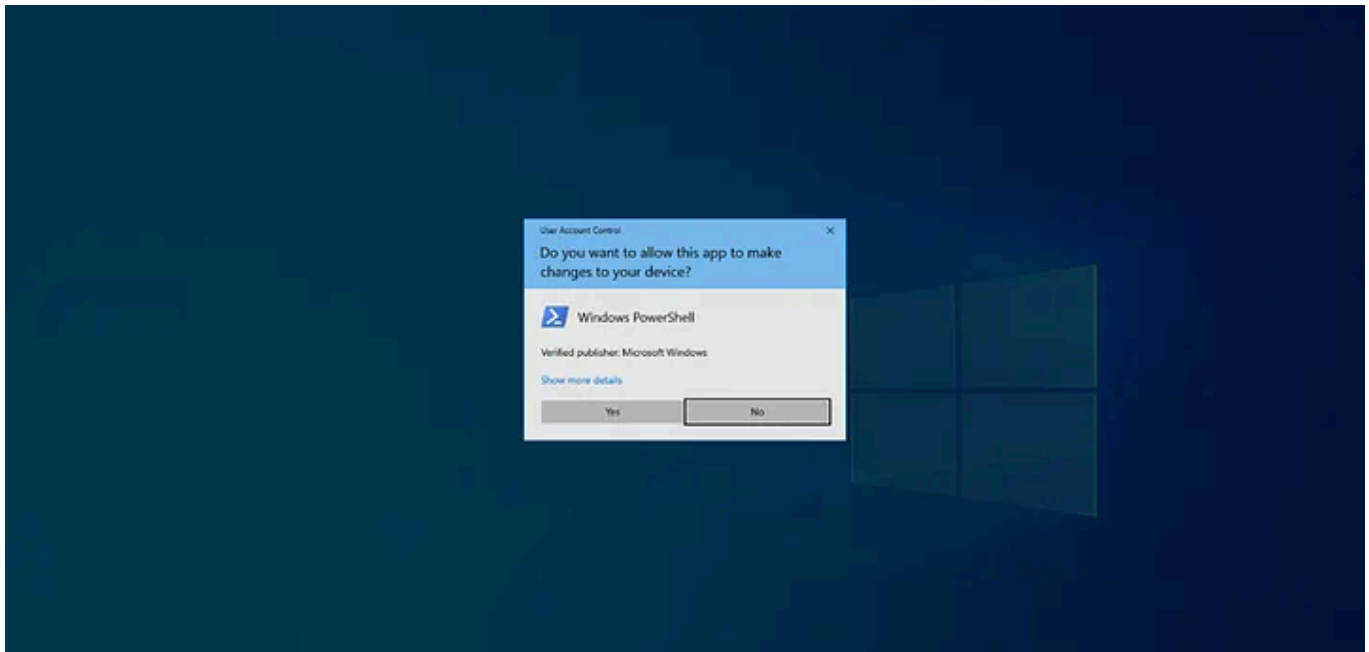


Fig. 7

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

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).

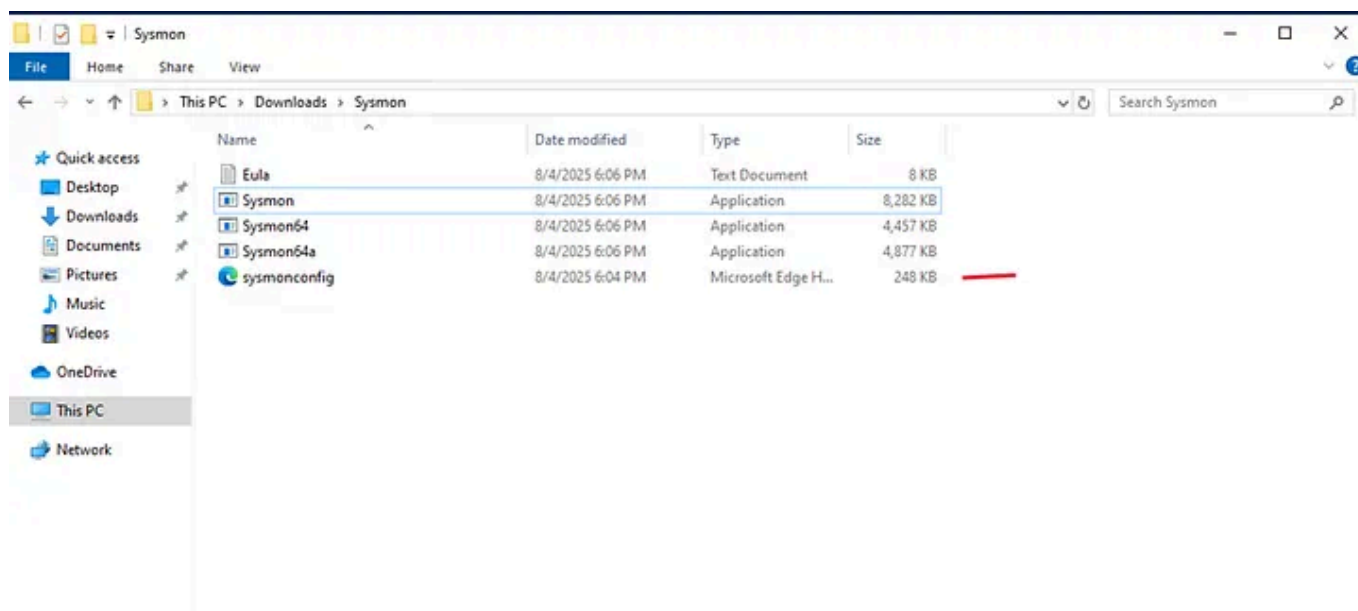


Fig. 9

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).


```
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> .\Sysmon64.exe

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install: Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema: Sysmon64.exe -s
Uninstall: Sysmon64.exe -u [force]
-c Update configuration of an installed Sysmon driver or dump the
  current configuration if no other argument is provided. Optionally
  take a configuration file.
-i Install service and driver. Optionally take a configuration file.
-m Install the event manifest (done on service install as well)).
-s Print configuration schema definition of the specified version.
  Specify 'all' to dump all schema versions (default is latest)).
-u Uninstall service and driver. Adding force causes uninstall to proceed
  even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in the boot that the service will write to the event log when it starts.
On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are written to the System event log.
Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals website.
Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to accept it.
Neither install nor uninstall requires a reboot.

PS C:\Users\Frederick\Downloads\Sysmon>
```

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).

```
PS C:\Users\Frederick\Downloads\Sysmon> .\Sysmon64.exe -i .\sysmonconfig.xml
```

Fig. 11

System Monitor License Agreement



You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Print

Agree

Decline

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).

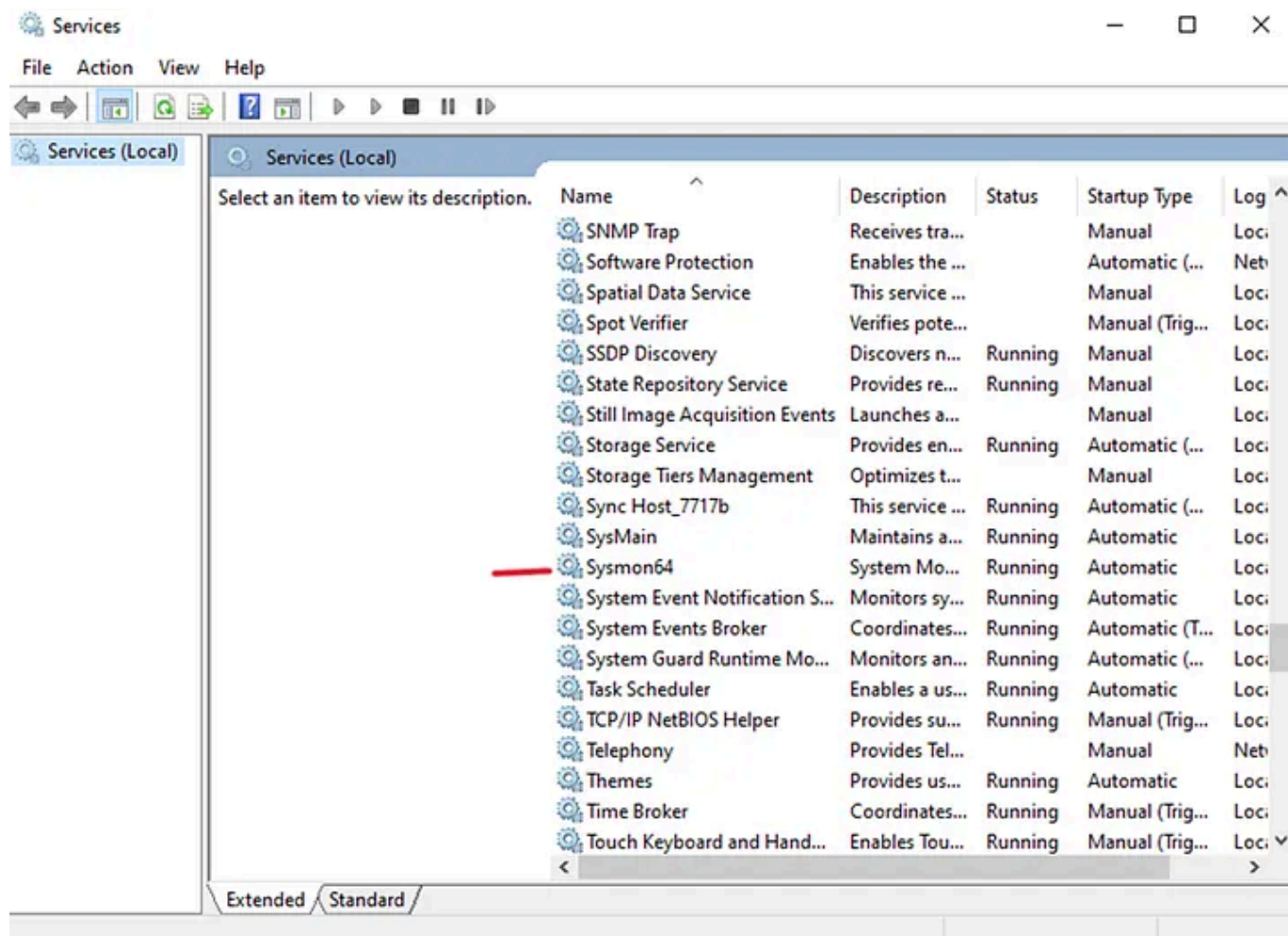


Fig. 13

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.

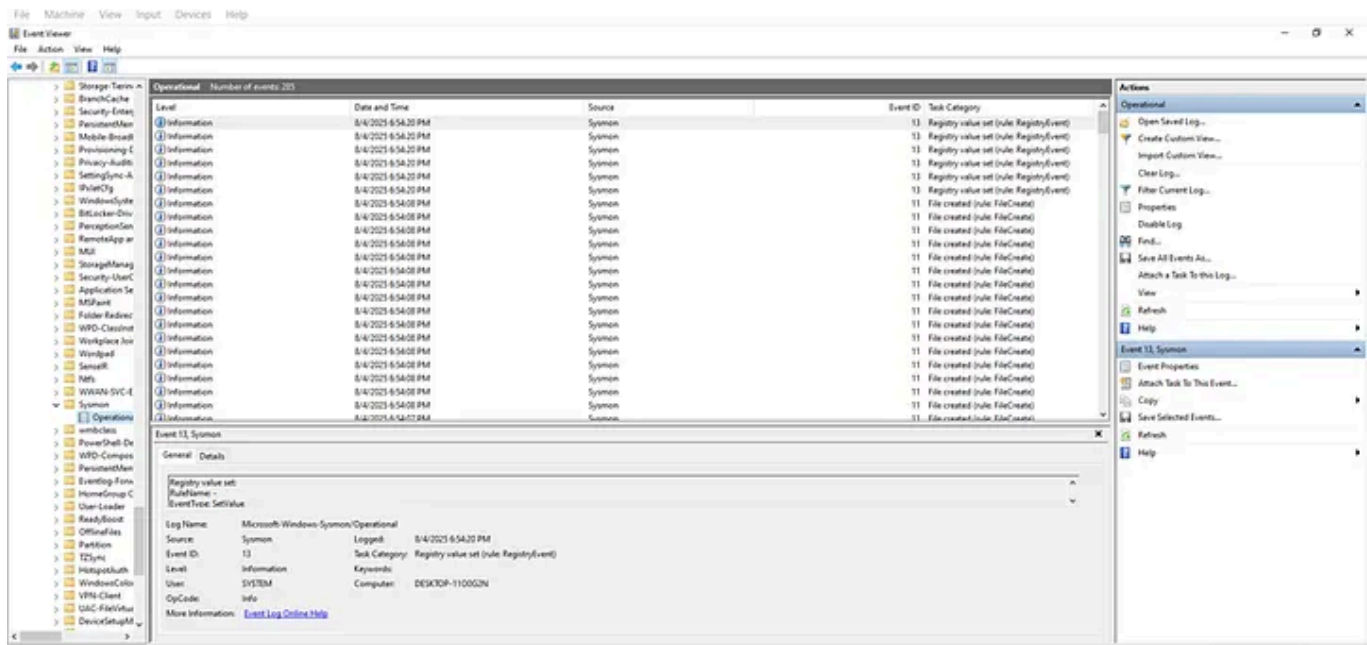


Fig. 14

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

**Written by Frederick Adigun**

3 followers · 2 following

[Edit profile](#)**No responses yet**

Frederick Adigun