

System Monitor

1. What is a Sysmon
2. Prerequisites
3. How to install Sysmon
4. Viewing the Sysmon logs
5. Benefits of Sysmon to security analysts

What is a Sysmon

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

Prerequisites

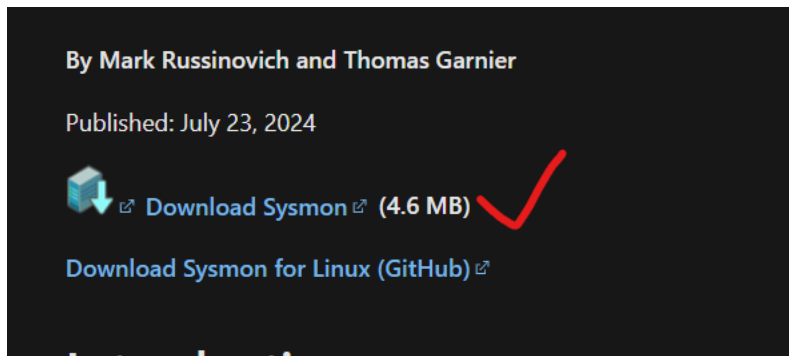
- ❖ Windows Host machine with admin rights
- ❖ 7 zip or winrar

How to install Sysmon



- ❖ Click on the link attached below and scroll down.

[Sysmon - Sysinternals](#) | [Microsoft Learn](#)

- ❖ Click download



- ❖ This will go directly to your download folder. Since its zipped, we will need to unzip it using the 7 zip app.

Name	Date modified	Type	Size
▼ Today			
 Sysmon	10/11/2024 11:02	Compressed (zipped)...	4,753 KB
 Sysmon	10/11/2024 11:04	File folder	

- ❖ Open PowerShell in admin mode and navigate to the folder where you stored the unzipped files of sysmon.

```
Administrator: C:\Program Files\WindowsApps\Microsoft.PowerShell_7.4.6.0_
PS C:\Users\Rose Wambui\Downloads\Compressed\Sysmon>
```

- ❖ Now that you are in the Sysmon directory, you will be able to install the app, to do this, run the following command:

```
PS Downloads\Compressed\Sysmon> .\Sysmon.exe -accepteula -i

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

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

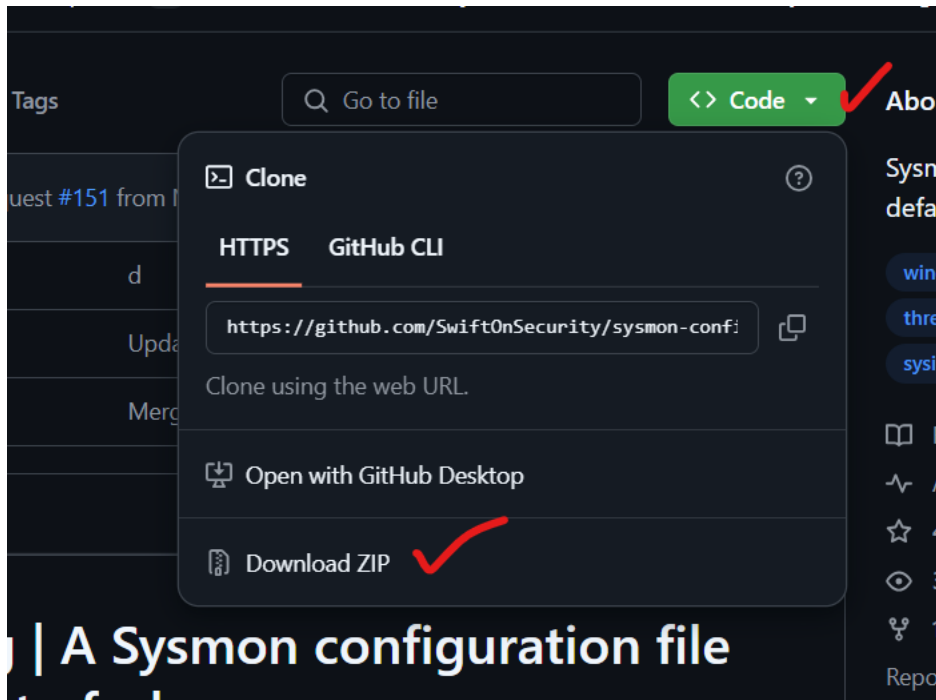
- ❖ Once this command has finished executing, Sysmon is now installed and you should be able to see the service running if you open the Services application:



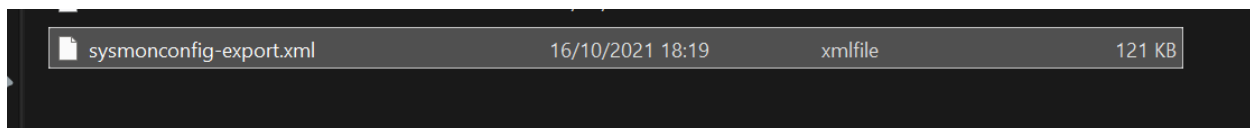
Sysmon being installed as is, doesn't really do much. To truly leverage this tool, we are going to need to use a config file. There are many config files for Sysmon available online, but for this tutorial I am going

to use SwiftOnSecurity's config file from GitHub (GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing) as it is recommended by multiple cyber security companies. Head to that link and download the files as a zip file.

- ❖ Click on the github link and download the files.



- ❖ Once the download has finished, extract the zip file.
- ❖ The folder will be named Sysmon-config-master. Open that folder and moved the file named "sysmonconfig-export.xml" to the Sysmon file



- ❖ We should have the following files in the Sysmon folder:

Name	Date modified	Type	Size
Earlier this year			
Sysmon	23/07/2024 14:08	Application	8,282 KB
Sysmon64	23/07/2024 14:08	Application	4,457 KB
Sysmon64a	23/07/2024 14:08	Application	4,877 KB
Eula	23/07/2024 14:08	Text Document	8 KB
A long time ago			
sysmonconfig-export.xml	16/10/2021 18:19	xmlfile	121 KB

❖ Now, head back to your PowerShell terminal and enter the following command:

```
PS [redacted]\Compressed\Sysmon> sysmon.exe -c sysmonconfig-export.xml

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

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated. ✓
Configuration updated. ✓
```

❖ The final step is to ensure that the config file has been applied. We are going to run the following command:

```
PS C:\Users\Rose Wambui\Downloads\Compressed\Sysmon> sysmon.exe -c

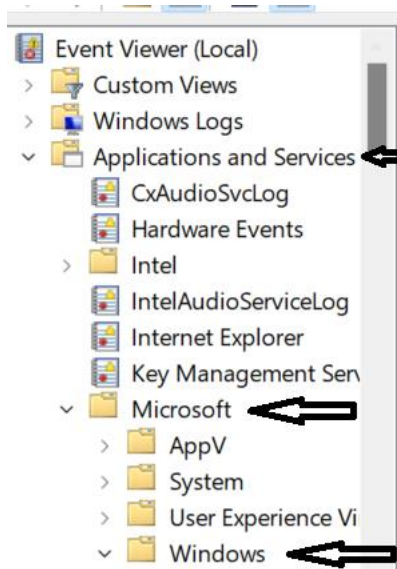
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
```

Assuming the output of this command was a huge list of query names and target objects, the configuration has been applied and the setup is complete. Sysmon can now be used for System Information and Events management including with the use of a SIEM tool.

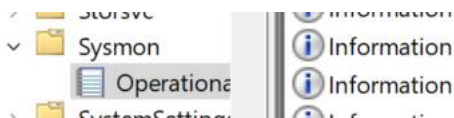
Viewing the Sysmon logs

Sysmon logs events to the Windows Event Log, specifically under “Applications and Services Logs” -> “Microsoft” -> “Windows” -> “Sysmon”.

❖ Search for the event viewer in the search and open it. Navigate to the Sysmon logs.



- ❖ After clicking on windows, scroll down until you find Sysmon.



Benefits of Sysmon to security Analysts

Detailed System Activity Monitoring: Sysmon captures detailed information about system events such as process creation, network connections, file creation, registry modifications, DLL loads, and more. This helps analysts gain insight into system and network activity, enabling them to identify indicators of compromise (IOCs) and detect potentially malicious behavior¹.

Enhanced Visibility: Sysmon fills the visibility gap left by native Windows event logs by providing more detailed and useful information. For example, it logs process creation events with full command line and hash information, which is not available in native Windows logs³.

Customization and Configuration: Sysmon allows analysts to precisely configure what events to generate. This means they can focus on specific event types or exclude certain events, reducing noise and optimizing analysis efforts¹.

Integration with SIEM and Threat Intelligence: Sysmon logs can be easily ingested into Security Information and Event Management (SIEM) systems, enabling analysts to correlate and analyze the collected data. Additionally, Sysmon logs can be compared against known threat intelligence sources to identify potential indicators of compromise¹.

Real-time Monitoring and Forensic Analysis: Sysmon provides real-time monitoring and detailed logs that are crucial for forensic analysis during incident response investigations.

Detection of Stealthy Malware: Sysmon helps in detecting ultra-stealthy malware techniques, such as HandleKatz credential dumping, which might not be detected by traditional antivirus or EDR solutions.

Control Over Telemetry: Unlike Endpoint Detection and Response (EDR) solutions, Sysmon gives administrators control over their telemetry, allowing them to uncover visibility gaps more effectively.

References

[Installing and Configuring Sysmon on Windows Servers | WinServerPro](#)

[GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing](#)

[Sysmon - Sysinternals | Microsoft Learn](#)

[Sysmon for Windows 11: A Comprehensive Guide | by SamRao | Medium](#)