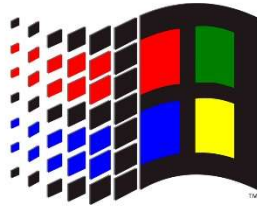
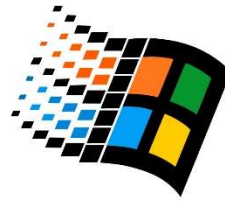


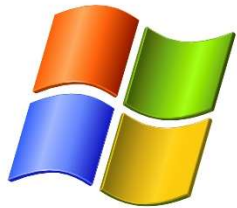
1985



1990



1995



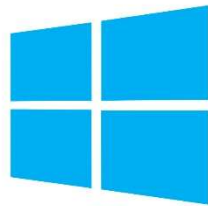
2001



2006-2009



2006



2012



Microsoft

# Sysmon

Mahesh Pavaskar

# Content



1. What is Sysmon?
2. Purpose of Sysmon / why?
3. Understand Sysmon few EventID
4. Download Sysmon
5. Installation of Sysmon
6. Check logs of sysmon in EventViewer
7. Swiftonsecurity - Sysmon config file
8. Update sysmon configuration

## What is Sysmon?



- URL : <https://learn.microsoft.com/en-us/sysinternals/downloads/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. It provides detailed information about process creations, network connections, and changes to file creation time.
- OR
- Sysmon (short for System Monitor) is part of the [Sysinternals software package](#), a set of free tools intended to troubleshoot, diagnose, manage and monitor Windows environments.

## Purpose of Sysmon / why?



- Extends Windows Logging Capabilities
- Detect Indicators of Compromise
- Sysmon Provides a Breadcrumb Trail

IMP URL : <https://www.blumira.com/sysmon-benefits/>

## Understand Sysmon few EventID



- **Event ID 1: Process creation**
- **Event ID 2: A process changed a file creation time**
- **Event ID 3: Network connection**
- **Event ID 4: Sysmon service state changed**
- **Event ID 5: Process terminated**
- **Event ID 6: Driver loaded**
- **Event ID 7: Image loaded**
- **Event ID 11: FileCreate**
- **Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)**
- **Event ID 22: DNSEvent (DNS query)**
- **Event ID 23: FileDelete (File Delete archived)**

## Download Sysmon



<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

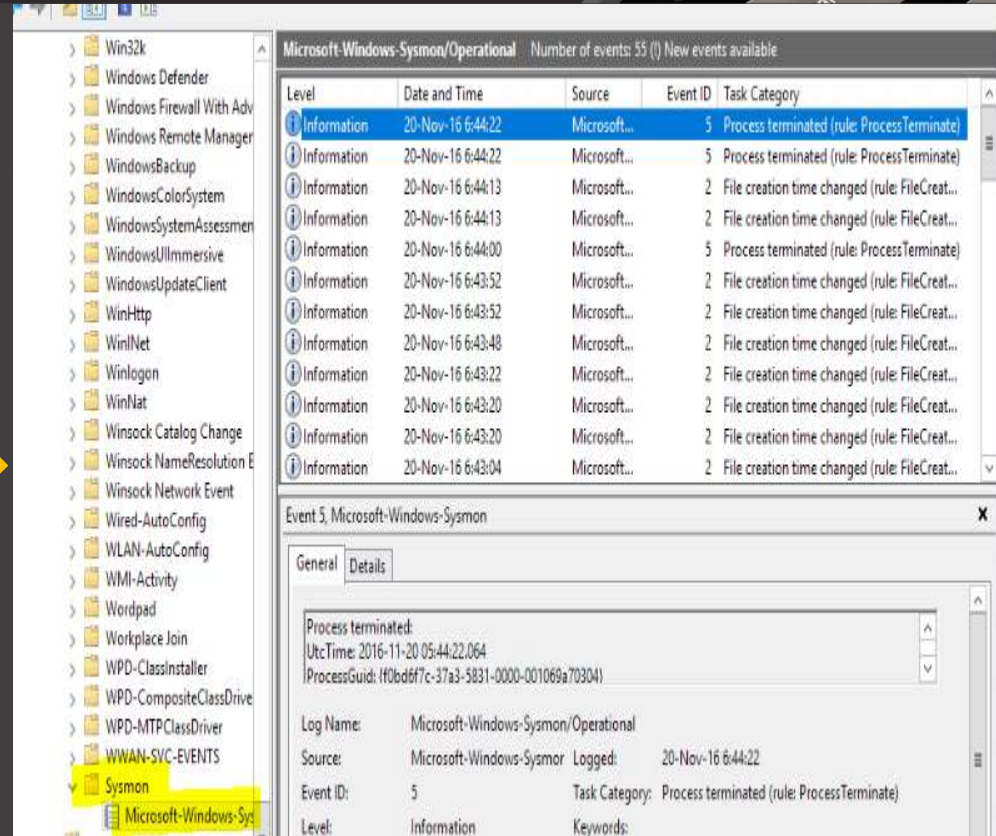
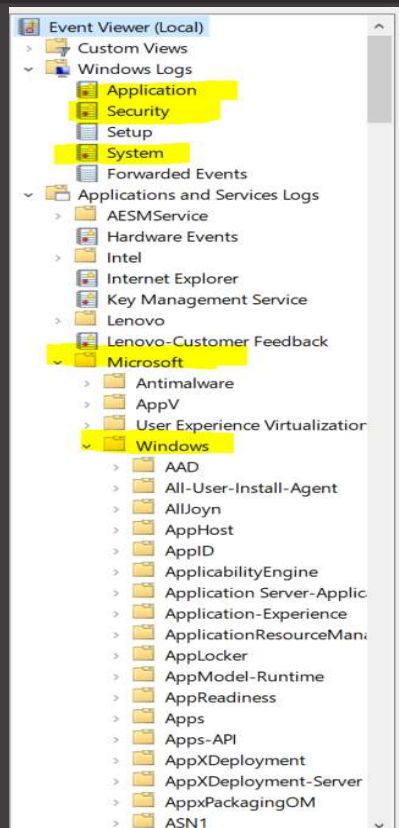
## Installation of Sysmon



Install with default settings (process images hashed with SHA1 and no network monitoring)

```
# sysmon64.exe -accepteula -i
```

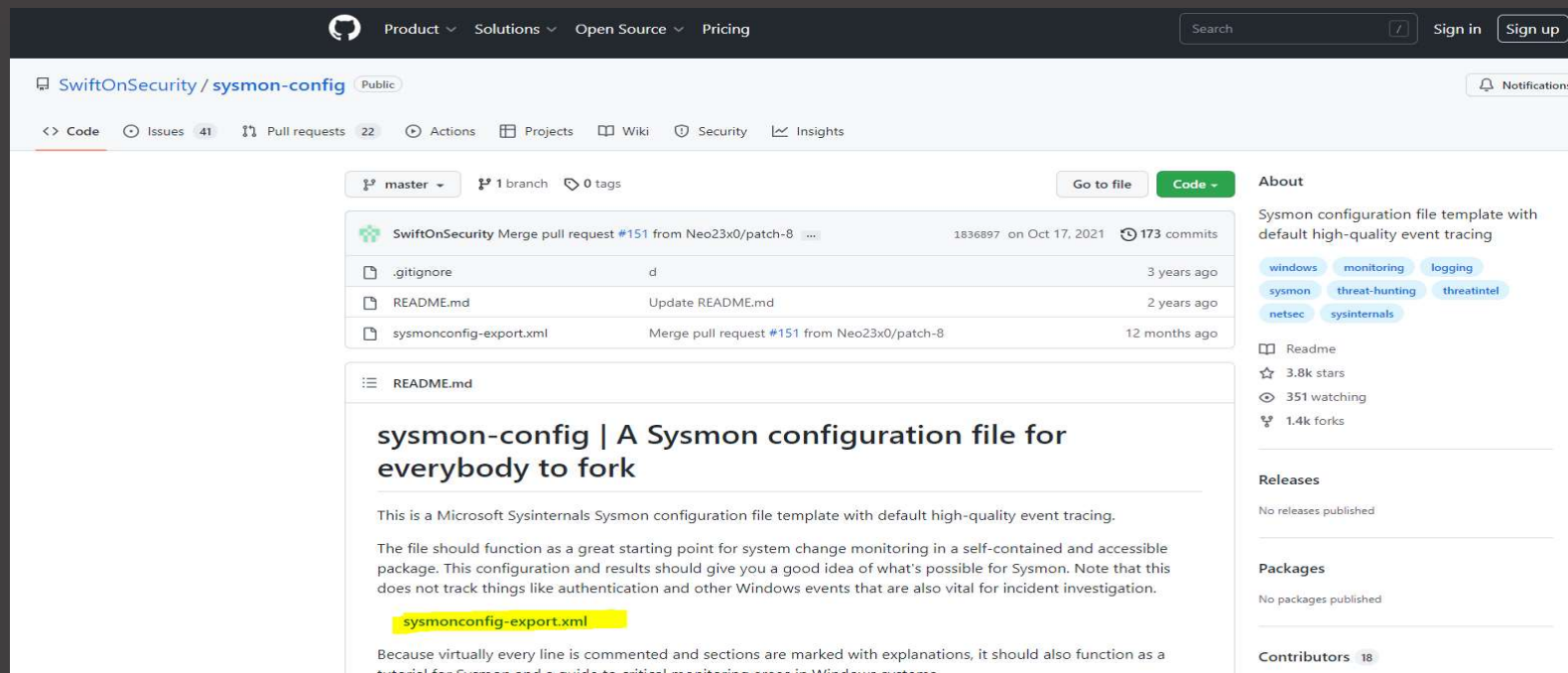
# Check logs of sysmon in EventViewer





# Swiftonsecurity - Sysmon config file

<https://github.com/SwiftOnSecurity/sysmon-config>



SwiftOnSecurity / **sysmon-config** Public

<> Code Issues 41 Pull requests 22 Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

SwiftOnSecurity Merge pull request #151 from Neo23x0/patch-8 1836897 on Oct 17, 2021 173 commits

File	Commit	Time
.gitignore	d	3 years ago
README.md	Update README.md	2 years ago
sysmonconfig-export.xml	Merge pull request #151 from Neo23x0/patch-8	12 months ago

README.md

## sysmon-config | A Sysmon configuration file for everybody to fork

This is a Microsoft Sysinternals Sysmon configuration file template with default high-quality event tracing.

The file should function as a great starting point for system change monitoring in a self-contained and accessible package. This configuration and results should give you a good idea of what's possible for Sysmon. Note that this does not track things like authentication and other Windows events that are also vital for incident investigation.

**sysmonconfig-export.xml**

Because virtually every line is commented and sections are marked with explanations, it should also function as a tutorial for Sysmon and a guide to critical monitoring areas in Windows systems.

**About**

Sysmon configuration file template with default high-quality event tracing

tags: windows, monitoring, logging, sysmon, threat-hunting, threatintel, netsec, sysinternals

Readme

3.8k stars

351 watching

1.4k forks

**Releases**

No releases published

**Packages**

No packages published

**Contributors** 18

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

## Update sysmon configuration

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





Thank you