OST

Eastern Switzerland
University of Applied Sciences

Sysmon

Windows Monitoring

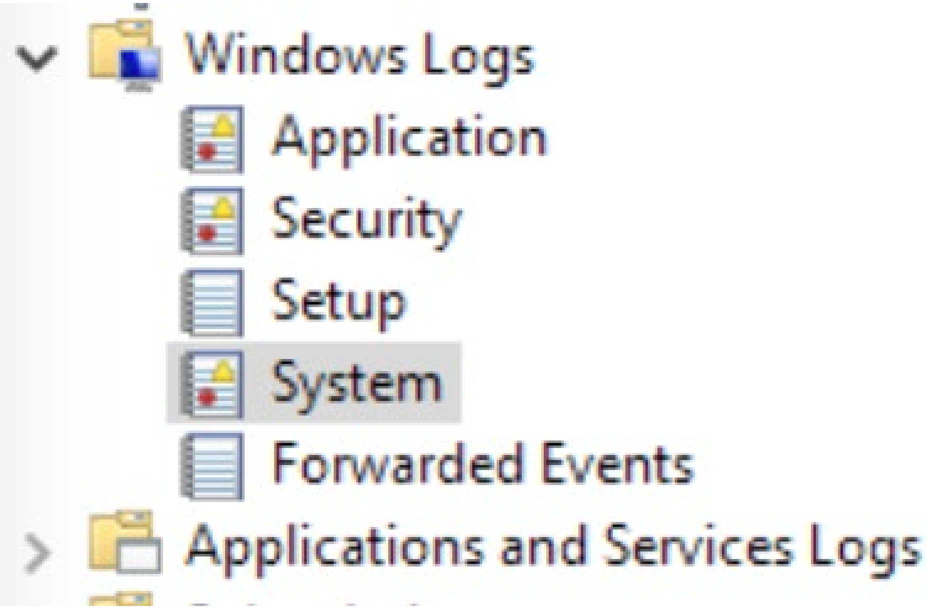
Ivan Bütler

3 December 2024

Departement of Informatics

Windows Logs

- Application log
  - Information about applications
- System
  - System component events
  - Driver issues, hardware issues…
- Security
  - Resource use
  - Logins/logoffs
  - File access



- Also will find a lot under Applications and Services Logs

“Sexy Six” event logs

- 4688/592 (Security) – New Process executed
  - Malware or malicious software running, or malicious actor running things
  - Not every new process is bad!!
  - Nmap.exe, ssh.exe, psexec.exe, psexecsvc.exe, ping.exe, powershell.exe, etc…
- 4624/528/540 (Security) – Account logged in
  - Attacker logged in
  - But not all logins are attackers!
  - 4625 – Failed logon attempt
- 5140/560 (Security) – A share was accessed
  - Accessing another computer
  - Lateral movement

“Sexy Six” event logs

- 5156 (Security) – Windows Firewall Network connection by process
  - See a process making a connection
  - Command and control maybe?
- 7045/601 (System) – New Service installed
  - New services generally should only be installed during patches and new software installation
  - Change management procedures – helps anomalies stand out
- 4663/567 (Security) – File and Registry auditing
  - Modifications to the system
  - Files added
  - Must enable file auditing

Some additional logs

- 4720 (Security) – A user account was created
  - Attackers could create themselves an account as a backdoor
  - Should be fairly easy to deconflict with the admin team
- 4732/4728 (Security) - A member was added to a group
  - Attackers could add their account to a higher privileged account
  - Should be fairly easy to deconflict with the admin team

Logon Types

- You’ll find these in logon events
- Most common…

- 2 – Logon via console
- 3 – Network logon
- 4 – Batch logon
- 5 – Windows service logon
- 10 – Remote interactive logon (RDP)

Process Auditing

- So not everything being audited in 4688 by default…
- gpedit.msc
- Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Detailed Tracking
- Audit Process Creation

Enable Command Line Auditing

- gpedit.msc
- Computer Configuration -> Administrative Templates -> System -> Audit Process Creation
- Include command line in process creation events
  - Enable

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.
- Free!
- A part of the Sysinternals Suite
- Created by Mark Russinovich
- Windows service and driver
- Monitoring + logging only – no analysis
  - Up to you + another tool to do that

Sysmon Event IDs

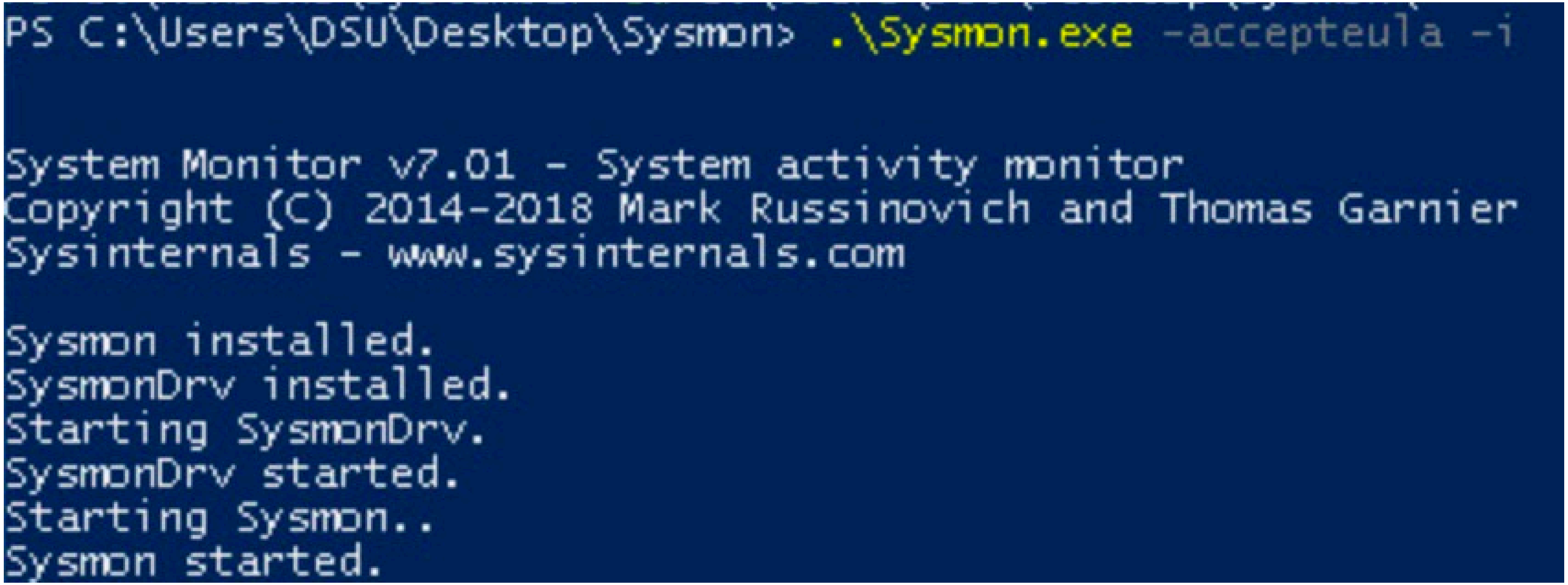
- 1 – Process creation
- 2 – A process changed a file creation time
- 3 – Network connection
- 4 – Sysmon service state changed (sysmon was started or stopped)
- 5 – Process terminated
- 6 – Driver loaded
- 7 – Image loaded (module is loaded in a process)
- 11 – FileCreate
- 12 – Registry Event (Create and Delete)
- Full list here: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon v15.11

Article • 11/13/2023 • 10 contributors

Installing Sysmon

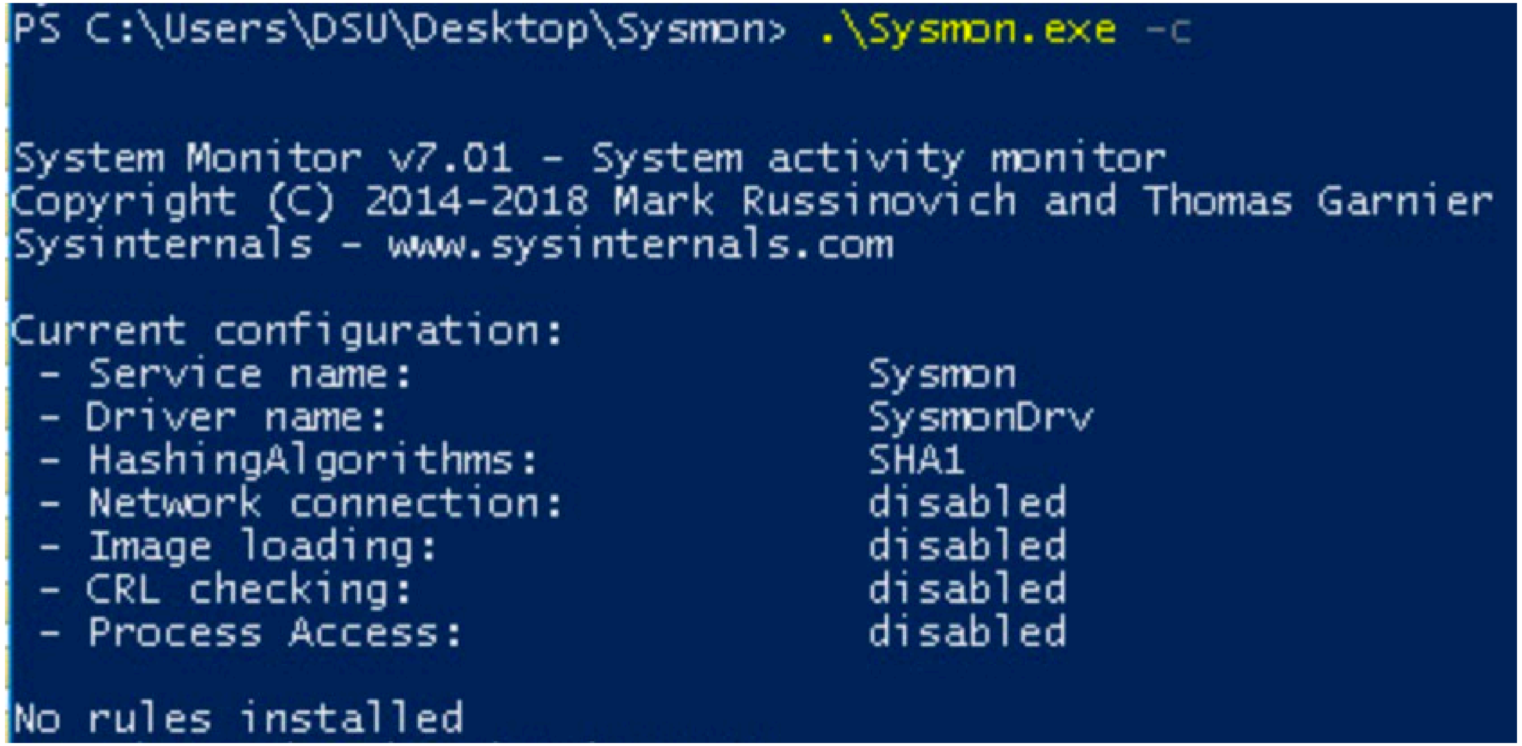
- Sysmon.exe -accepteula –i
  - Must install as an admin, since you are installing a service



```
PS C:\Users\DSU\Desktop\Sysmon> .\Sysmon.exe -accepteula -i


System Monitor v7.01 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

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

Default Configuration

- Sysmon.exe –c
- Gets current configuration
  - Not a whole lot there…



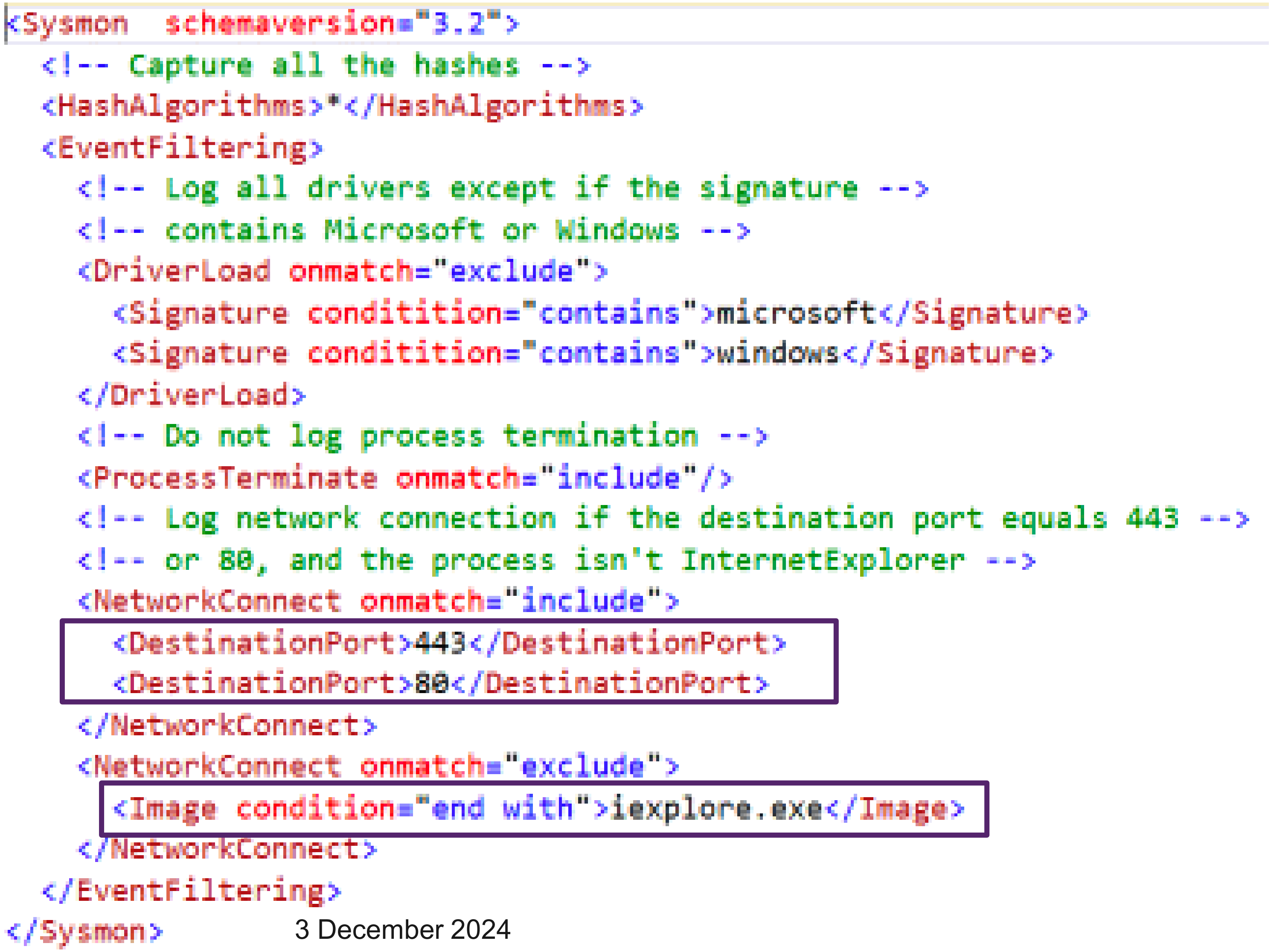
```
PS C:\Users\DSU\Desktop\Sysmon> .\Sysmon.exe -c


System Monitor v7.01 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                  Sysmon
 - Driver name:                   SysmonDrv
 - HashingAlgorithms:             SHA1
 - Network connection:            disabled
 - Image loading:                 disabled
 - CRL checking:                  disabled
 - Process Access:                disabled

No rules installed
```

Filtering

- We can configure Sysmon to
  - Only show certain events (include)
  - Filter out certain events (exclude)
- Do I care to see every smss.exe event?
  - Is it malicious?
  - Probably not…
    - But make sure you only filter out the OFFICIAL path/executable!
  - Session Manager Subsystem – it's normal.
- XML configuration file
  - Include events that match…
  - Exclude events that match…

Sample Configuration File

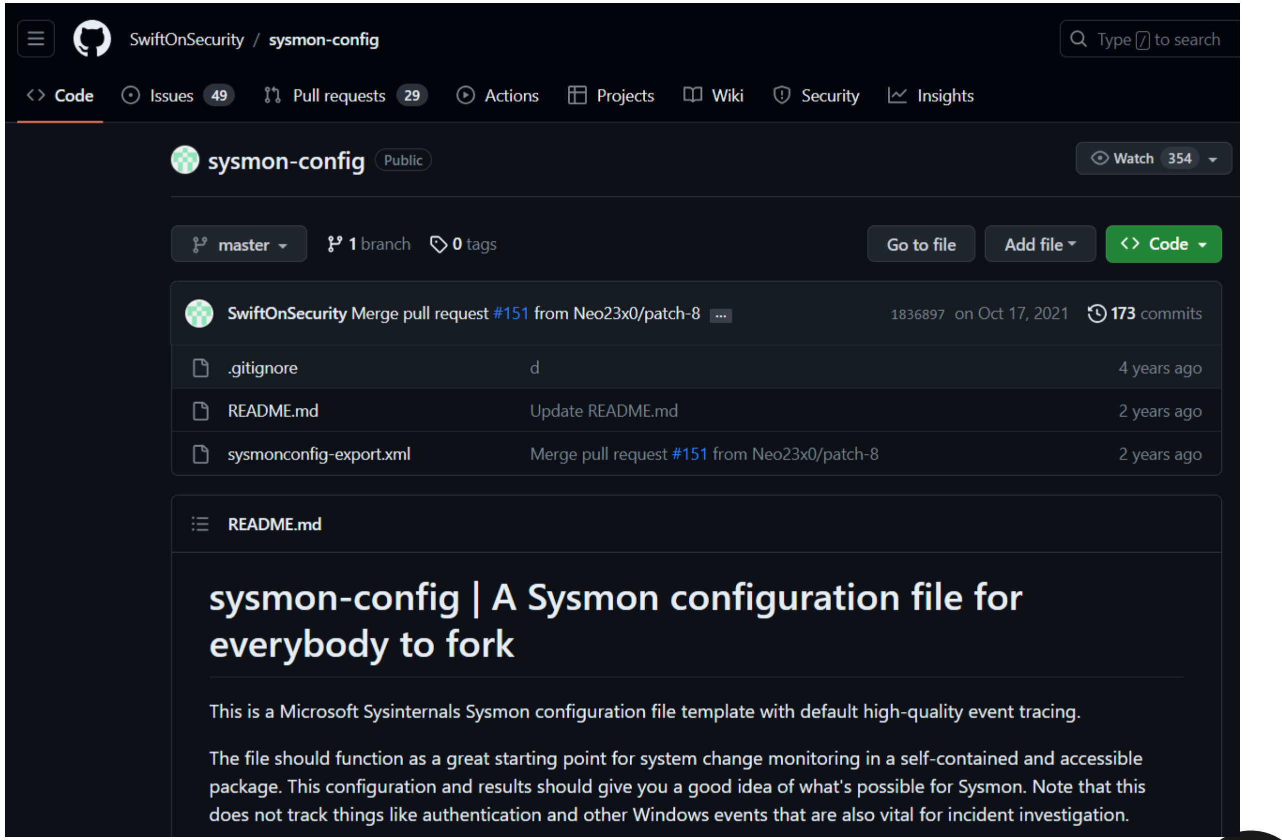
- Network
  - Only connections on ports 80 and 443 notfrom Internet Explorer
- Drivers
  - Exclude “Microsoft”
  - Exclude “windows”
- No process termination events



```
<Sysmon  schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condititition="contains">microsoft</Signature>
      <Signature condititition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

Filtering Templates

- SwiftOnSecurity Sysmon Configuration
  - https://github.com/SwiftOnSecurity/sysmon-config
- A good baseline to begin from
- 800+ lines
  - It’s long
  - But it’s good
- Tweak for your own organization



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

.gitignore	d	4 years ago
README.md	Update README.md	2 years ago
sysmonconfig-export.xml	Merge pull request #151 from Neo23x0/patch-8	2 years 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.

Tweaking the Config

- Logging EVERYTHING will get noisy
  - Think tons of events on thousands of computers in a large organization
  - Too much data to deal with
- Don’t want to exclude things that could be malicious
- Please – read through the sample config if you start there
  - Make sure you understand what you’re doing
  - Make sure you agree with what it’s doing
- Put it in play and see what happens
  - Some legitimate process making tons of logs on your network? Exclude it.
  - Afraid you’re not getting a full enough picture of something? Include it.