

Sysmon

Installation og opdatering af config samt
løbende opdateringer af Sysmon Config

Indholdsfortegnelse

Indledning.....	3
Installation.....	4
Opdatering af Sysmon Config.....	5
Løbende opdateringer af Config filen på Servers og klienter.....	5
Oprettelse af Sysmon update task.....	6

Indledning

Denne vejledning beskriver installation af Sysmon på Windows 11 25H2. Samt løbende opdateringer af Sysmon config filen.

3 årsage til man løbende bør opdatere sine Sysmon Config Filer.

- **Sikkerhed.** I forhold til sikkerhed, bliver nye hacker, malware metodikker tilføjet til config filen. Ved nye frigivet versioner af Sysmon fra Microsoft, kommer der typisk også nye ting man kan overvåge. Her bliver Sysmon Config filen tilpasset til de nye funktioner.
- **Log optimeringer.** For at holde antallet af logs nede på en niveau der ikke koster for meget at indsamle til SIEM systemer, bliver der optimeret på kun at indhente de nødvendige logs.
- **Licensforbrug.** Selve logopsamlingen fra klienter / servers koster i sig selv ikke andet end CPU forbruget og Internet forbindelsen, samt ca. 100Mb harddisk plads. For hele tiden at holde licensforbrug på et acceptabelt niveau, når dette skal opbevares og behandles på et SIEM system, optimeres der på hvor mange logs der modtages fra hosts.

Installation

Eksempel for installation af native Sysmon.

Download og udpak indholdet fra Sysmon zip filen fra Networkforensic til C:\Windows\Sysmon

Download herfra

<https://networkforensic.dk/Sysmon/default.html>

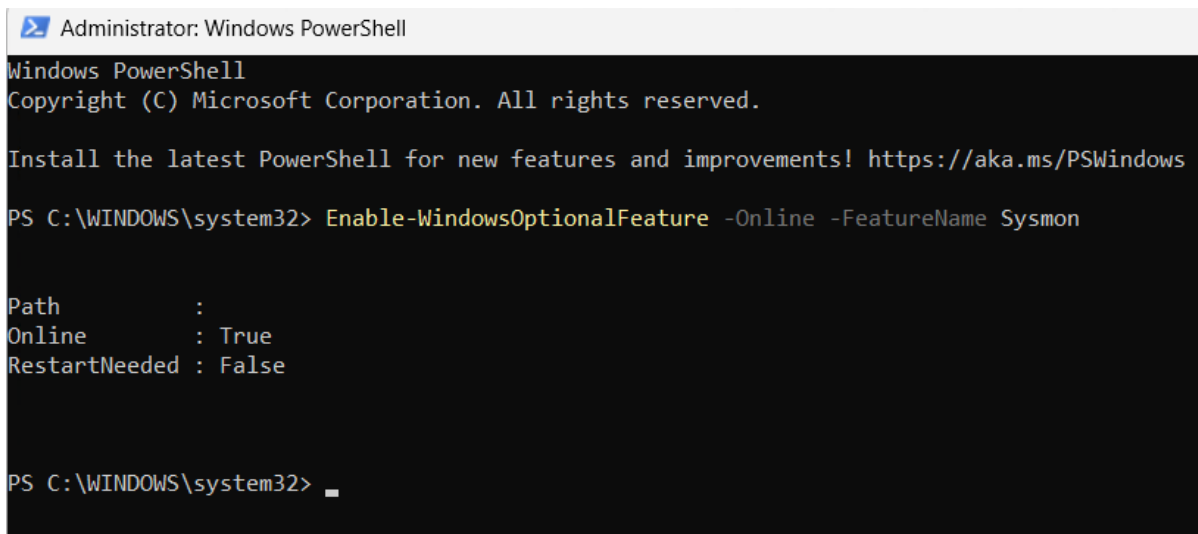
Opret eventuelt folderen "Sysmon" så du har C:\Windows\Sysmon med filerne heri.

Install Windows Sysmon feature fra en Powershell Command prompt

Start PowerShell med admin rettigheder.

Kør følgende command

Enable-WindowsOptionalFeature -Online -FeatureName Sysmon



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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Enable-WindowsOptionalFeature -Online -FeatureName Sysmon

Path           :
Online         : True
RestartNeeded : False

PS C:\WINDOWS\system32> _
```

Installer Sysmon

Naviger til C:\Windows\Sysmon

Med administrative rettigheder start "Install-Sysmon.cmd"

Ref links:

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/overview>

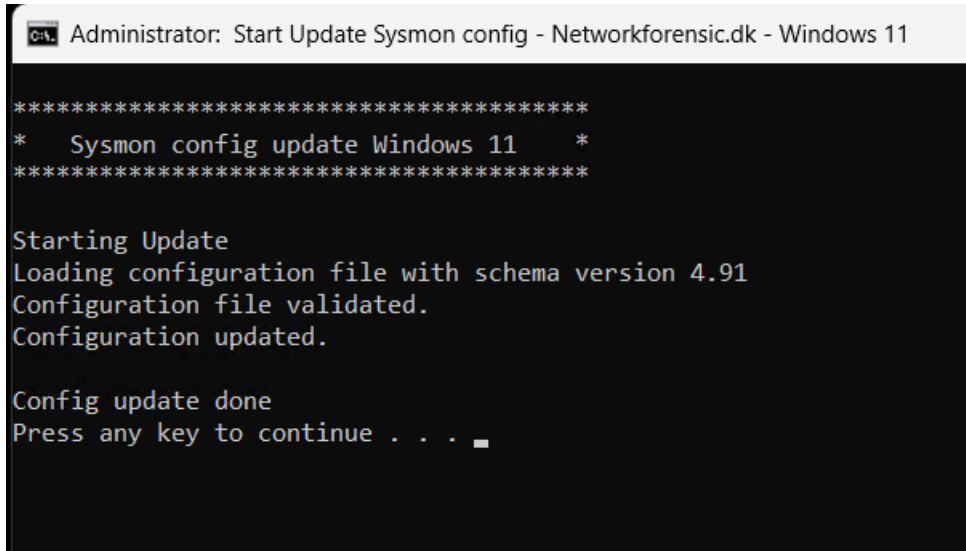
<https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/how-to-enable-sysmon>

Opdatering af Sysmon Config

Eksempel for manuel opdatering af Sysmon Config:

Naviger til C:\Windows\Sysmon

Med administrative rettigheder start "Update-Sysmon-Config.cmd"



```
Administrator: Start Update Sysmon config - Networkforensic.dk - Windows 11
*****
* Sysmon config update Windows 11 *
*****
Starting Update
Loading configuration file with schema version 4.91
Configuration file validated.
Configuration updated.
Config update done
Press any key to continue . . . _
```

Løbende opdateringer af Config filen på Servers og klienter

Et eksempel man kan benytte til løbende opdateringer af Sysmon Config filen er beskrevet herunder.

Når man har installeret Sysmon, ønsker man ofte en løbende opdatering til seneste config. Metoden her kan man selv lave og tilpasse som man ønsker, men metoden her kan benyttes som benytter et PowerShell Script for download og udpakning af Zip filen samt en opdatering af Config filen. Dette gøres med Task Scheduler på både klienter og servers. Dette samlet vil hente den seneste frigivet Sysmon Config fra Networkforensic og opdatere Sysmon Config filen på klienter ellers Servers.

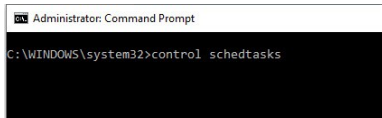
Løsningen her virker både på interne og eksterne systemer som eks laptops der er uden for ens netværk. Den virker også på standalone systemer og i AD miljøer.

Har man fulgt vejledningen for installation af Sysmon og har oprettet C:\Windows\Sysmon med tilhørende filer. Så ligger der i "Task" folderen 3 typer XML filer der kan importes direkte i Task Scheduler, alt efter om det er en klient eller en server. Denne import kræver administrative rettigheder. Man kan selv vælge at tilpasse dette til egne miljøer, så det passer ens egne ønsker.

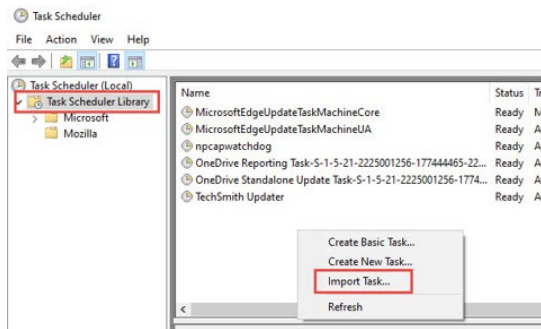
Oprettelse af Sysmon update task

Eksempel på en import på en klient.

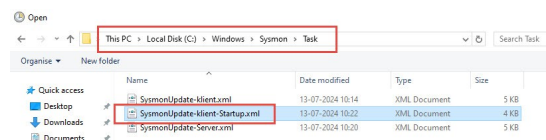
1 – Åben en Command Promt med administrative rettigheder kørs ”control schedtasks”



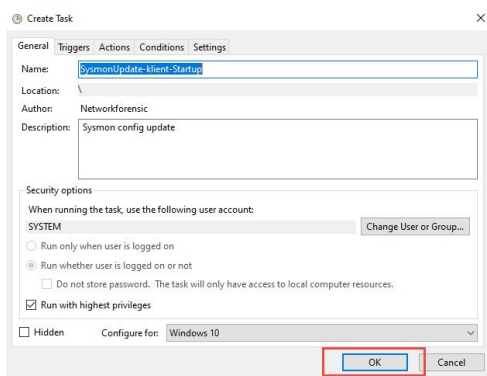
2 – Højreklik og vælg – ”Import Task”



3 – Naviger til C:\Windows\Sysmon\task – vælg ”SysmonUpdate-klient-Startup.xml”



4 – Vælg ”OK”



5 – Automatiks opdatering er nu oprettet og klienten vil nu hente den seneste config ved hver opstart.

