Sysmon

Installation og opdatering af config samt
løbende opdateringer af Sysmon Config

Indholdsfortegnelse

Indledning

Denne vejledning beskriver installation af Sysmon 15.15 med config. 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 Sysinternals, 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. Vi oplever at mange af de gratis Sysmon config der kan hentes andre steder på Internettet slet ikke har fokus på optimeret log indsamling. Dette kan blive en bekostelig affære at benytte i SIEM licenser.

- **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 of Sysmon:

Hint:
Disse filer virker kun såfremt at nuværende installeret Sysmon service hedder ”TaskhostView”. Eller hvis der er tale om en førstegangs installation. Hedder din installeret service noget andet skal dette tilrettes i ”Install-Sysmon.cmd” – ”Install-Sysmon.cmd” – ”Update-Sysmon-Config.cmd” med det service navn der er benyttet.

Udpak indholdet fra Sysmon zip filen fra Networkforensic til C:\Windows\Sysmon
Opret eventuelt folderen "Sysmon" så du har C:\Windows\Sysmon med filerne heri.

I en kommando promt med administrative rettigheder:
Naviger til C:\Windows\Sysmon og kør filen Install-Sysmon.cmd

Dette vil fjerne alle tidligere versioner og installerer nuværende Sysmon 15.15 med seneste config fil
Genstart af systemet er ikke nødvendig.

Afinstallation

Eksempel for afinstallation af Sysmon:

I en kommando promt med administrative rettigheder:
Naviger til C:\Windows\Sysmon og kør filen Uninstall-Sysmon.cmd
Genstart af systemet er ikke nødvendig.

Opdatering af Sysmon Config

Eksempel for opdatering af Sysmon Config:

I en kommando promt med administrative rettigheder:
Naviger til C:\Windows\Sysmon og kør filen Update-Sysmon-Config.cmd
Genstart af systemet er ikke nødvendig.

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.

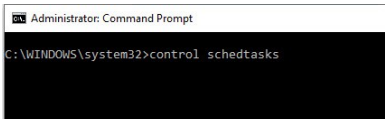
Løsningen her virker både på interne og eksterne systemer som eks laptops der er uden for ens netværk. Den virker også på standalone systemer og i AD miljøer.

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.

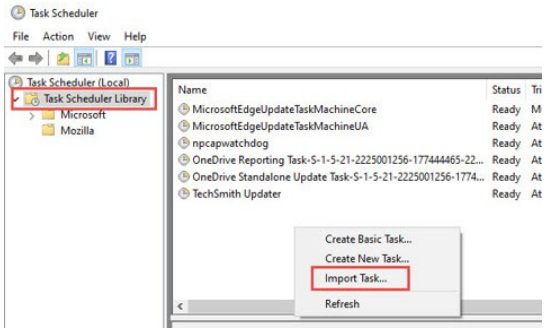
Oprettelse at Sysmon update task

Eksempel på en import på en klient.

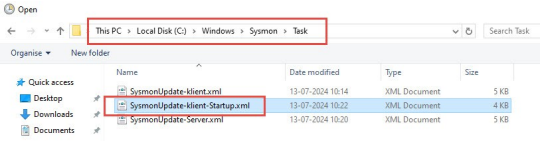
1 – Åben en Command Promt med administrative rettigheder kør ”control schedtasks”



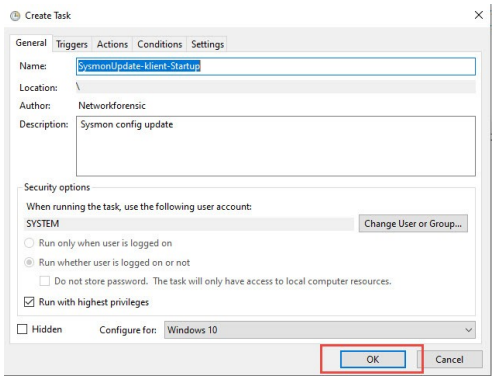
2 – Højreklik og vælg – “Import Task”



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.