Øvelse – Udvidet logning med Sysmon

Information

Windows Event Logs giver en grundlæggende indsigt i systemhændelser.
Dog registrerer standard Windows logs ikke alle aktiviteter, som kan være relevante i en sikkerhedsundersøgelse.

Sysmon (System Monitor) er et værktøj fra Microsoft Sysinternals, som udvider Windows logging.

Sysmon installerer en Windows-service, der overvåger systemaktivitet og registrerer detaljerede hændelser i **Windows Event Log**.

Sysmon kan blandt andet registrere:

- procesopstart
- netværksforbindelser
- oprettelse af filer
- ændringer i registry
- procesrelationer (parent/child processes)

Disse logs bruges ofte i:

- **incident response**
- **threat hunting**
- **digital forensics**

Sysmon registrerer forskellige typer hændelser ved hjælp af **Event IDs**.

Eksempler:

Event ID	Betydning
1	Process creation
3	Network connection
11	File creation

I denne øvelse skal du installere Sysmon og undersøge de logs, som værktøjet genererer.

Instruktioner

1 Download Sysmon

Download Sysmon fra Microsoft Sysinternals:

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

Udpak zip-filen på serveren.

Der skal udforskes lidt her. Hvor downloader, og udpakker man direkte i powershell?

2 Installer Sysmon

I **PowerShell som administrator**, navigér til mappen hvor Sysmon ligger.

Installer Sysmon med standardkonfiguration:

```
.\Sysmon64.exe -i
```

Bekræft installationen når du bliver spurgt.

---

3 Kontrollér at Sysmon kører

Kør følgende kommando:

```
Get-Service Sysmon64
```

Spørgsmål

1. Kører Sysmon-servicen?
2. Hvilken status har servicen?

---

4 Find Sysmon logs

Sysmon skriver logs til Windows Event Log.

Loggen findes her:

```
Microsoft-Windows-Sysmon/Operational
```

Vis de seneste events:

```
Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 20
```

Vis de første events via pipeline:

```
Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Select -First
10
```

Spørgsmål

1. Hvor mange events kan du se?
2. Hvilke Event IDs optræder?

---

5 Undersøg procesopstart

Sysmon registrerer procesopstart med **Event ID 1**.

Kør følgende kommando:

```
Get-WinEvent -FilterHashtable @{
    LogName="Microsoft-Windows-Sysmon/Operational"
    Id=1
} -MaxEvents 10 | Format-List
```

Spørgsmål

1. Hvilke processer er startet?
2. Hvilken proces startede dem (Parent Process)?

Procesrelationer kan være meget vigtige i en sikkerhedsundersøgelse, da de kan vise hvordan programmer startes af andre programmer.

---

6 Generér nye events

Start nogle programmer eller kommandoer på systemet.

Eksempel:

```
notepad
ipconfig
whoami
```

Kør derefter igen:

```
Get-WinEvent -FilterHashtable @{
    LogName = "Microsoft-Windows-Sysmon/Operational"
    Id      = 1
} -MaxEvents 10 | Select-Object TimeCreated, Id, Message | Format-List
```

Spørgsmål

1. Kan du finde events der svarer til de kommandoer du har kørt?
2. Hvilken information giver Sysmon om processerne?

Refleksionsspørgsmål

1. Hvilke typer aktiviteter kan Sysmon registrere som ikke findes i standard Windows logs?
2. Hvorfor kan procesrelationer (parent/child processes) være vigtige i en sikkerhedsundersøgelse?
3. Hvilke fordele kan der være ved at installere Sysmon på en server i en organisation?
4. Hvordan kunne Sysmon hjælpe med at opdage malware eller kompromitterede systemer?

Links

Sysmon – Microsoft Sysinternals download

Sysmon documentation

Sysmon event IDs reference

Get-WinEvent PowerShell documentation

Last update: 2026-03-20 13:58:28