

451 - WINDOWS

Audita tu propio PC con Sysmon de Microsoft

Registra qué programas se ejecutan en tu Windows y aprende a detectar actividad sospechosa como hacen los equipos de seguridad.



NIVEL
Avanzado

TIEMPO
30 min

CATEGORÍA
Windows

WEB
soporteinformatico360.com

Sysmon es una herramienta gratuita de Microsoft que apunta en un registro todo lo que se ejecuta en tu equipo. Con ella aprenderás a mirar tu propio PC como lo haría un analista de seguridad y a descubrir programas que no esperabas.

■ Qué necesitas

- ✓ Un PC con Windows 10 u 11 que sea tuyo
- ✓ Una cuenta de administrador
- ✓ Sysmon descargado de la web oficial de Microsoft
- ✓ Unos 30 minutos

■ Paso a paso

01

Descarga Sysmon

Búscalo en la sección Sysinternals de learn.microsoft.com, descarga el ZIP y descomprímelo en una carpeta, por ejemplo C:\Herramientas\Sysmon.



02

Abre la terminal como administrador

Pulsa Win + X y elige Terminal (Administrador).
Acepta el aviso de Control de cuentas.



03

Instálalo

Entra en la carpeta y ejecuta la instalación. Sysmon se queda funcionando como servicio y no ralentiza el equipo.

Terminal

```
$ cd C:\Herramientas\Sysmon
$ sysmon64 -accepteula -i
$
```

04

Mira lo que registra

Abre el Visor de eventos y entra en el registro de Sysmon. El evento 1 indica cada programa que se inicia, con su ruta y quién lo lanzó.

Visor de eventos

Registros de aplicaciones y servicios

Microsoft > Windows > Sysmon

Operational

05

Haz una prueba

Abre el Bloc de notas y busca en el registro el evento 1 con notepad.exe. Así aprendes a seguir el rastro de un programa.

06

Desinstálalo si ya no lo quieres

Cuando termines de practicar, puedes quitarlo desde la misma terminal de administrador con sysmon64 -u.

■ Consejos

CONSEJO 1

Revisa sobre todo programas que se ejecutan desde Descargas o Temp: es donde suele esconderse el malware.

CONSEJO 2

Existen configuraciones públicas de Sysmon más completas; léelas antes de aplicarlas con sysmon64 -c.

CONSEJO 3

Sysmon solo registra, no bloquea: mantén Microsoft Defender activo.



Importante: Úsalo solo en equipos tuyos o con permiso. Vigilar o atacar sistemas ajenos sin autorización es delito. Si no te ves con ello, pide ayuda a un técnico.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112