Incidentes de ciberseguridad

SYSMON

Jennifer

Indicaciones

En equipos servidor y en estaciones de trabajo donde se guarde información confidencial es importante monitorizar adecuadamente el sistema y guardar registros de todo lo que pasa, o al menos de lo más importante.

En los sistemas Windows existe una herramienta creada por Microsoft llamada sysmon .

System Monitor (Sysmon) es un servicio que una vez instalado permanece activo siempre para supervisar y registrar la actividad del sistema en el registro de sucesos de Windows.

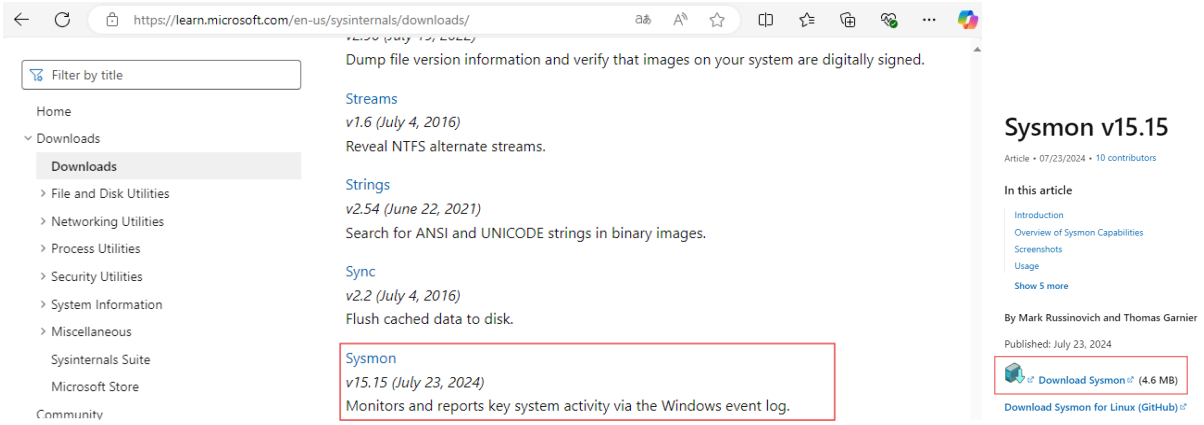
Sysmon puede registrar sucesos de:

- Procesos que se crean.
- Conexiones de red.
- Cambios en el registro.
- Comandos que se ejecutan.
- Instalar, configurar, monitorizar y analizar los LOGs generados por sysmon.

Requisitos previos

1. Windows 7,8,10 (32 o 64 bits)
2. Sysinternals suite (https://docs.microsoft.com/en-us/sysinternals/downloads/)
3. Fichero de configuración (https://github.com/SwiftOnSecurity/sysmon-config)
4. Sysmon Tools (https://github.com/nshalabi/SysmonTools)

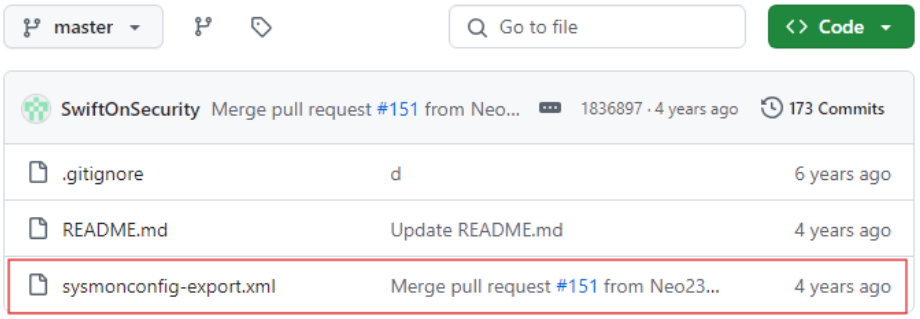
- **Descargate la utilidad sysmon (2)**
  1. Para ello descargo e instalo SYSMON con la usl que me facilitaron



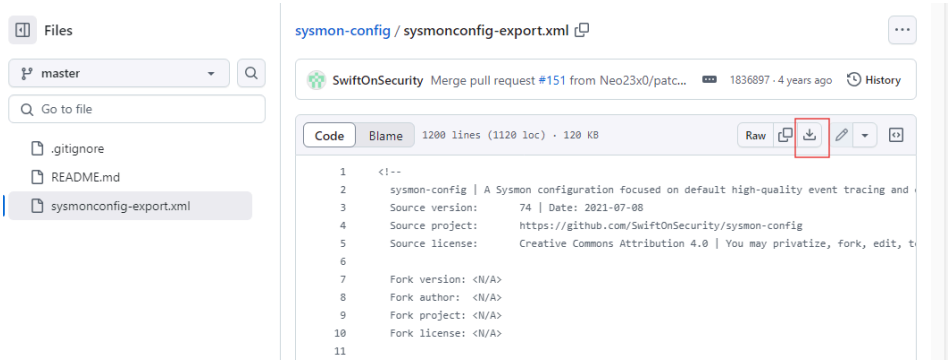
  2. Desencripto el archivo descargado

- **Descargate el fichero de configuración (3)**

1. Con el URL que me proporcionó el profe descargo el fichero xml para la configuración de SYSMON



2. Lo descargo



Entender un poco el contenido del fichero de configuración.

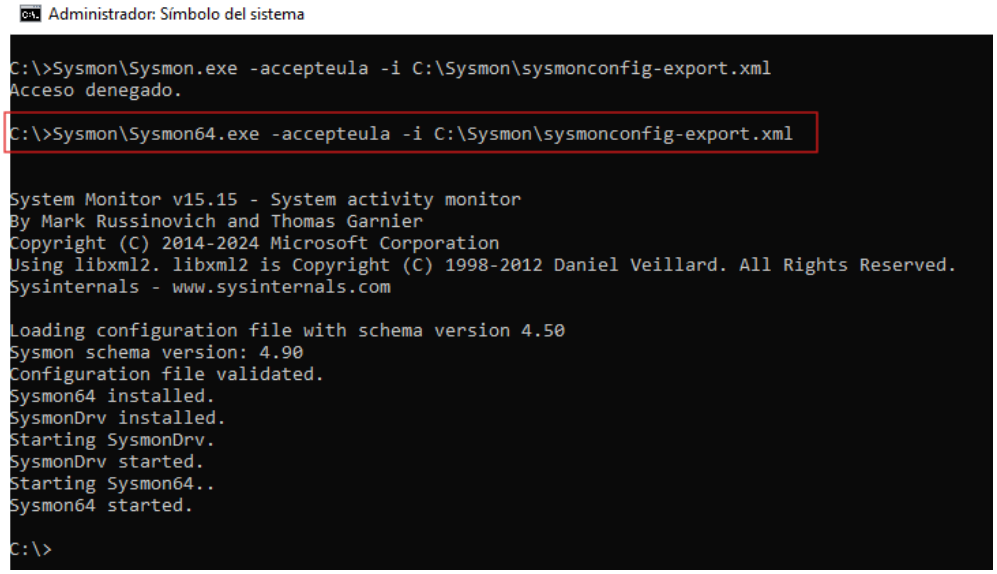
El fichero XML de configuración de Sysmon (System Monitor) es el archivo donde se define las reglas y filtros que dicta cómo este monitor de sistema de Microsoft recopila y registra eventos en la máquina o red la estructura básica del archivo se encuentran varios ID que son:

- <!--SYSMON EVENT **ID 1** : PROCESS CREATION [ProcessCreate]--> **Creación de procesos**
- <!--SYSMON EVENT **ID 3** : NETWORK CONNECTION INITIATED [NetworkConnect]--> **Conexión de red iniciada**
- <!--SYSMON EVENT **ID 4** : RESERVED FOR SYSMON SERVICE STATUS MESSAGES→ **Mensajes de estado reservados para el servicio Sysmon.**
- <!--SYSMON EVENT **ID 5** : PROCESS ENDED [ProcessTerminate]--> **Terminación de procesos**
- <!--SYSMON EVENT **ID 6** : DRIVER LOADED INTO KERNEL [DriverLoad]--> **Carga de un controlador en el kernel**
- <!--SYSMON EVENT **ID 7** : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]--> **Carga de una DLL (imagen) por un proceso**
- <!--SYSMON EVENT **ID 8** : REMOTE THREAD CREATED CreateRemoteThread]--> **Creación de un hilo remoto en un proceso**
- <!--SYSMON EVENT **ID 9** : RAW DISK ACCESS [RawAccessRead]--> **Acceso a disco en modo crudo**
- <!--SYSMON EVENT **ID 10** : INTER-PROCESS ACCESS [ProcessAccess]--> **Acceso entre procesos**

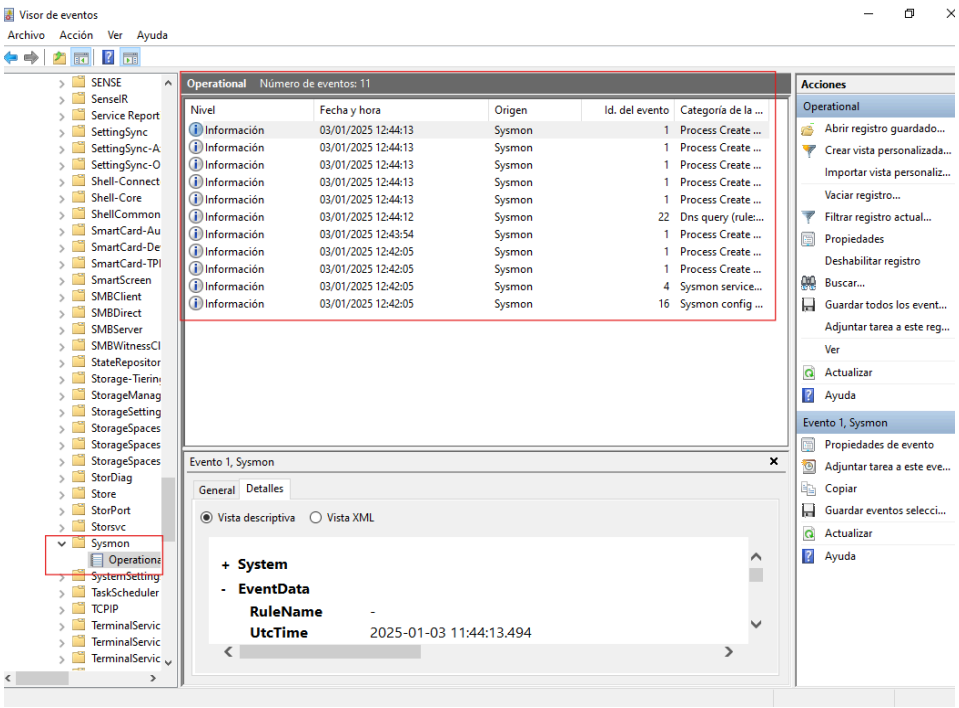
- <!--SYSMON EVENT **ID 11** : FILE CREATED [FileCreate]--> **Creación de un archivo**
- <!--SYSMON EVENT **ID 12 & 13 & 14** : REGISTRY MODIFICATION [RegistryEvent]-->
    - <!--EVENT **12**: "Registry object added or deleted"--> **Objeto del Registro añadido o eliminado**
    - <!--EVENT **13:** "Registry value set"--> **Valor del Registro establecido**
    - <!--EVENT **14**: "Registry objected renamed"--> **Objeto del Registro renombrado**
- <!--SYSMON EVENT **ID 15** : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]--> **Creación de flujos alternativos de datos en archivos**
- <!--SYSMON EVENT **ID 16** : SYSMON CONFIGURATION CHANGE→ **Cambios en la configuración de Sysmon.**
- <!--SYSMON EVENT **ID 17 & 18** : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    - <!--EVENT **17**: "Pipe Created"--> **Creación de un pipe**
    - <!--EVENT **18:** "Pipe Connected"--> **Conexión a un pipe**
- <!--SYSMON EVENT **ID 19 & 20 & 21** : WMI EVENT MONITORING [WmiEvent]-->
    - <!--EVENT **19:** "WmiEventFilter activity detected"--> **Actividad detectada en filtros de WMI**
    - <!--EVENT **20:** "WmiEventConsumer activity detected"--> **Actividad detectada en consumidores de WMI**
    - <!--EVENT **21**: "WmiEventConsumerToFilter activity detected"--> **Relación entre filtro y consumidor de WMI detectada**
- <!--SYSMON EVENT **ID 22** : DNS QUERY [DnsQuery]--> **Consulta DNS realizada**
- <!--SYSMON EVENT **ID 23** : FILE DELETE [FileDelete]--> **Eliminación de archivos**
- <!--SYSMON EVENT ID **23** : FILE DELETE [FileDelete]-->
    - <!--EVENT **24**: "Clipboard changed"--> **Cambios en el portapapeles**
- <!--SYSMON EVENT **ID 25** : PROCESS TAMPERING [ProcessTampering]--> **Manipulación de procesos detectada**
- <!--SYSMON EVENT **ID 255** : ERROR--> **Error del sistema o de Sysmon.**

Instalación servicio sysmon

1. Es importante que el archivo que nos descargamos este directamente en la unidad C:, para su instalación tenemos que usar el CMD con permisos de administrador utilizando el siguiente comando para su instalación dependiendo la version te pedirá uno u otro:
   C:\>Sysmon\Sysmon.exe -accepteula -i C:\Sysmon\sysmonconfig-export.xml

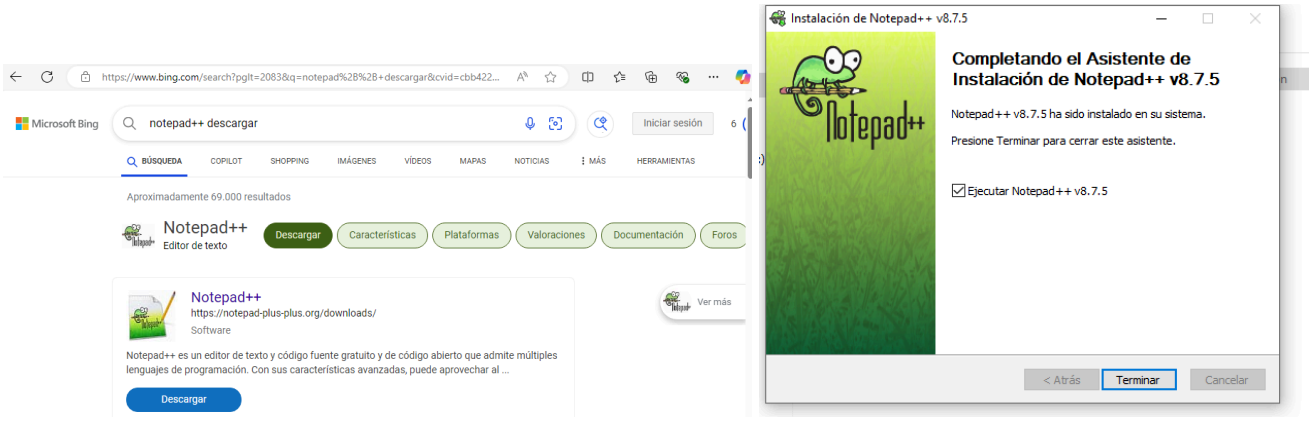


2. Una vez instalado, Sysmon se ejecuta en segundo plano, recogiendo información y escribiéndola en el Visor de Eventos de Windows.
   Para acceder al visor de eventos. Presionamos la tecla **window +R** y escribimos **eventvwr.msc**, En la parte izquierda buscamos en:
   Registro de aplicaciones/Microsoft/Windows/Sysmos

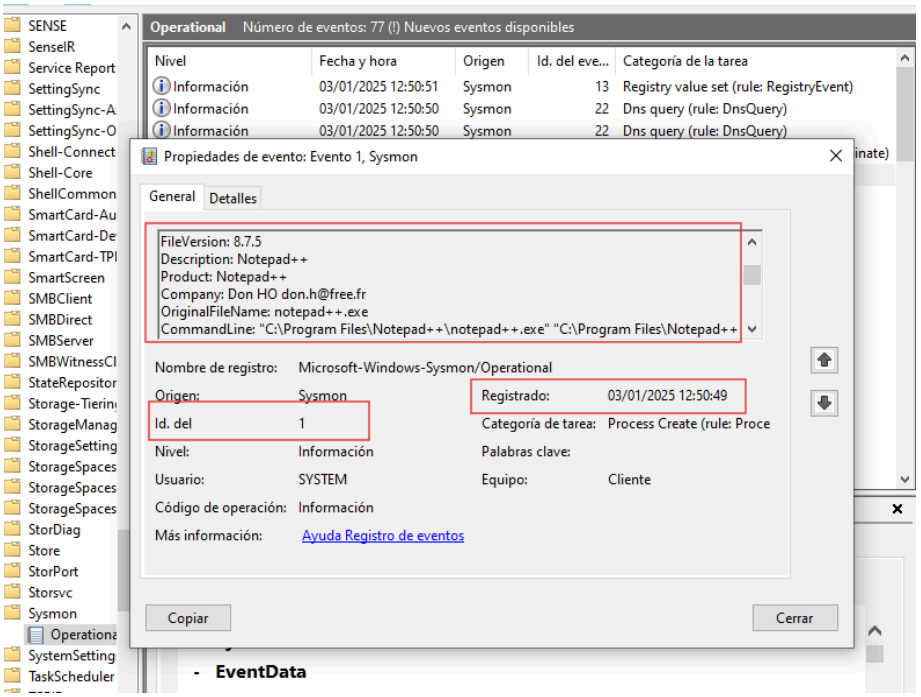


Ejemplo de uso

Descarge el software para verificar como se registra el evento.

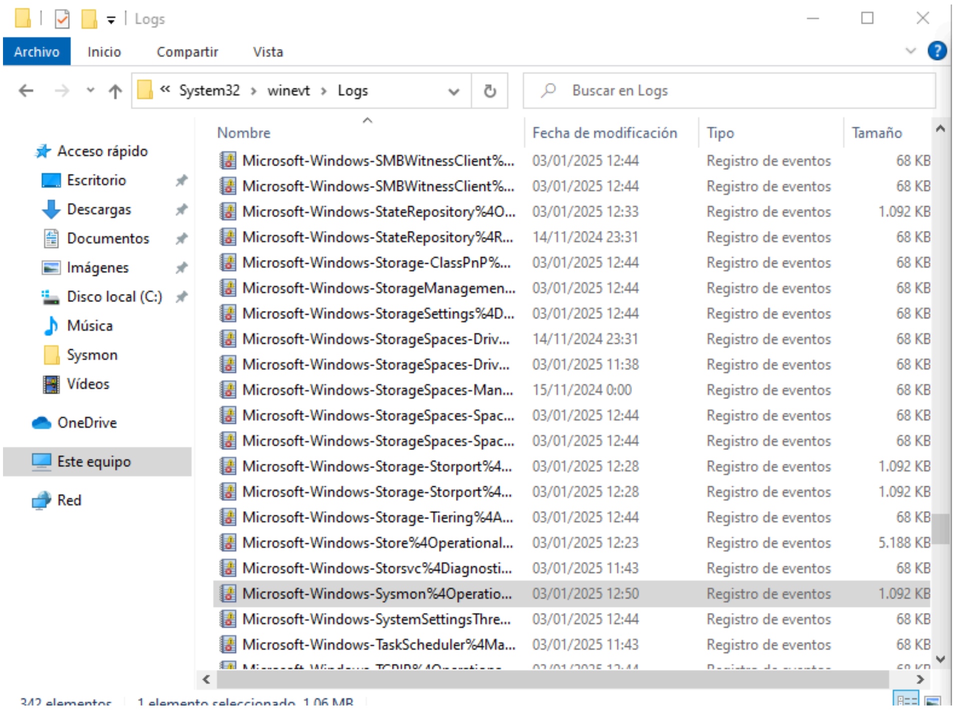


Podemos ver como se registró con el ID 1 se ve como se ejecutó el tipo de versión etc

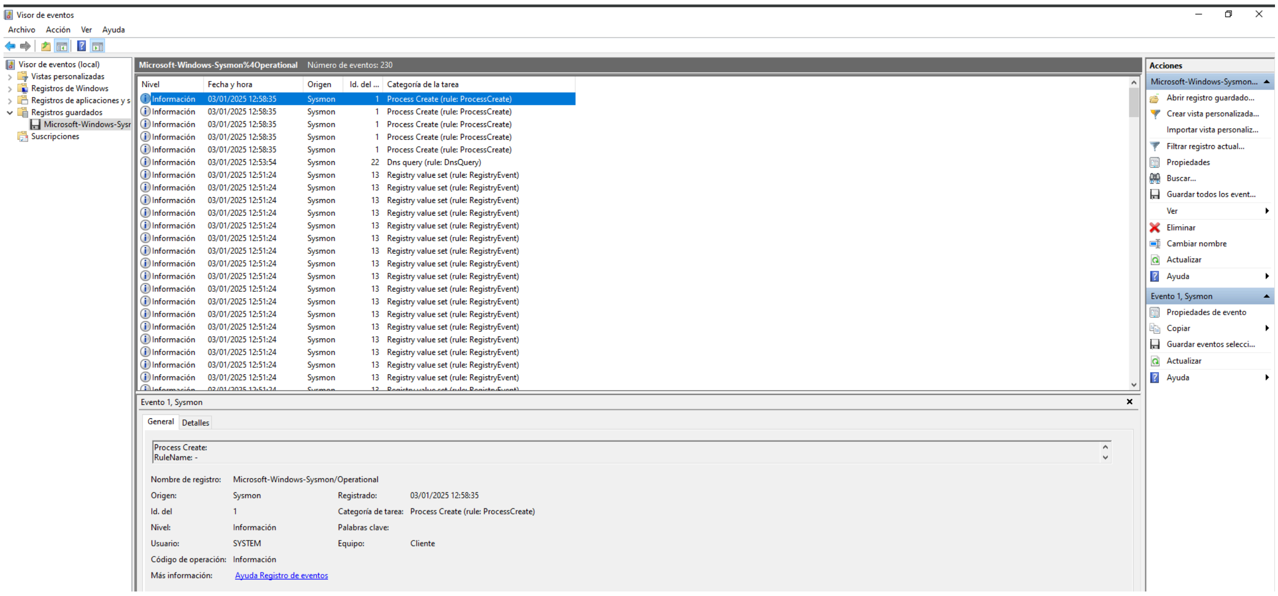


- La última parte de sysmon sería el análisis de la información que recoge.
  - Por defecto sysmon guarda los registros en el fichero de eventos en la siguiente ruta:

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx

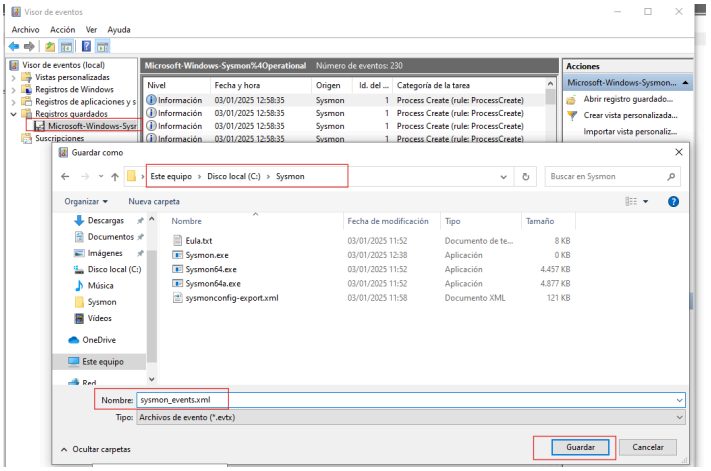


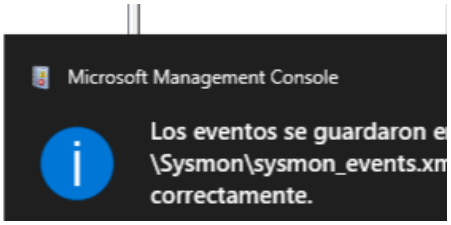
  - Abre el fichero con el " Visor de eventos "



○ Exporta el contenido del fichero a formato XML **(Menú contextual -> guardar todos los eventos como XML)**

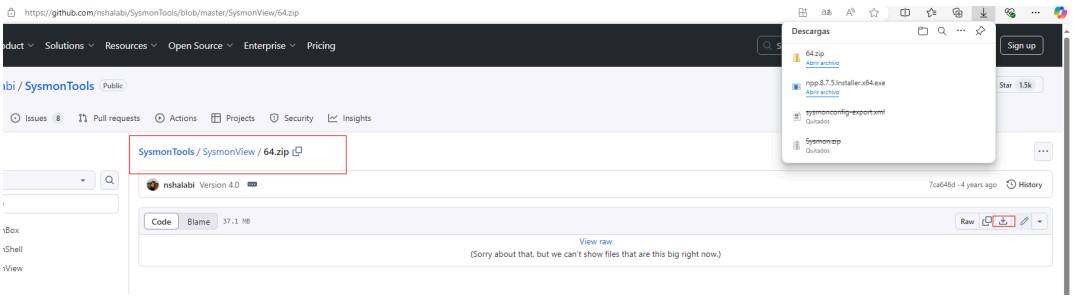
Seleccionamos guardar como



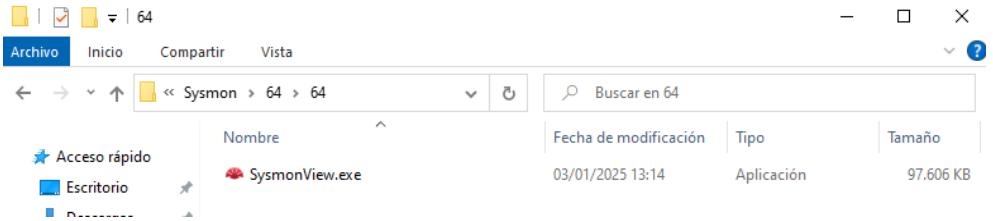


○ **Abre el fichero XML con la utilidad SysmonViewer y explora su funcionalidad.**

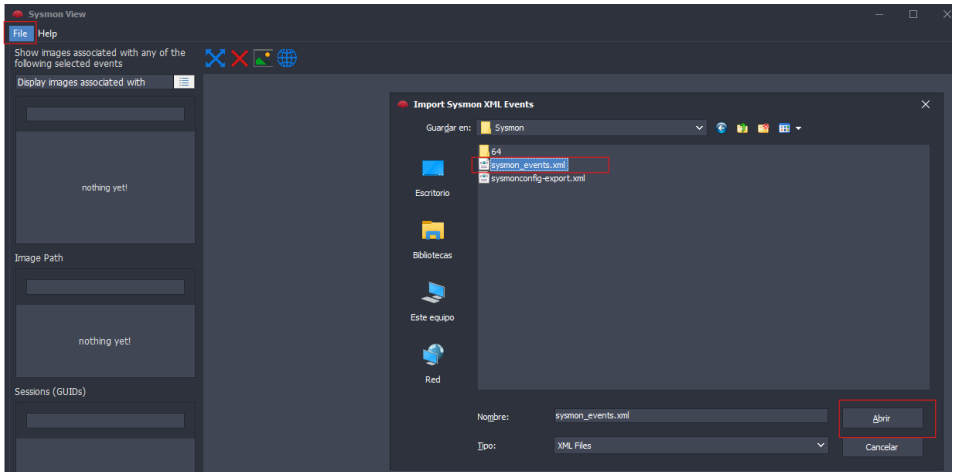
1. Instalo el software que nos pide Sysmon Tools me descargo el **SysmonViewer**



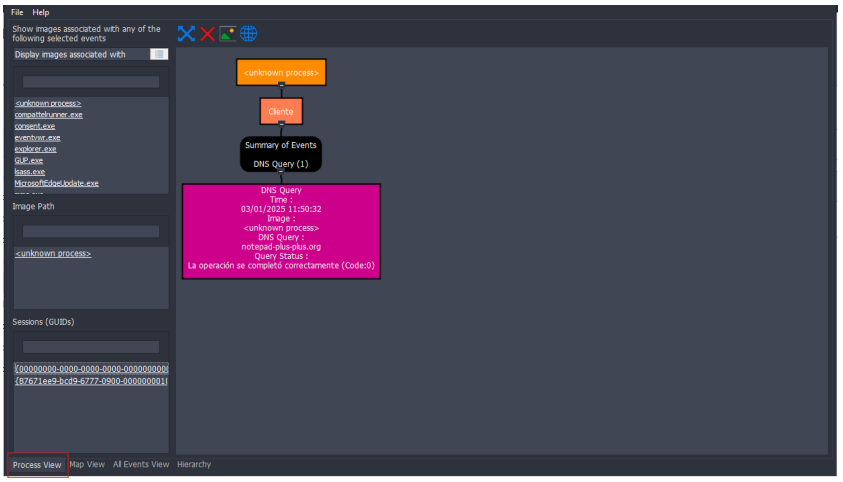
2. Lo instalo **SysmonViewer**



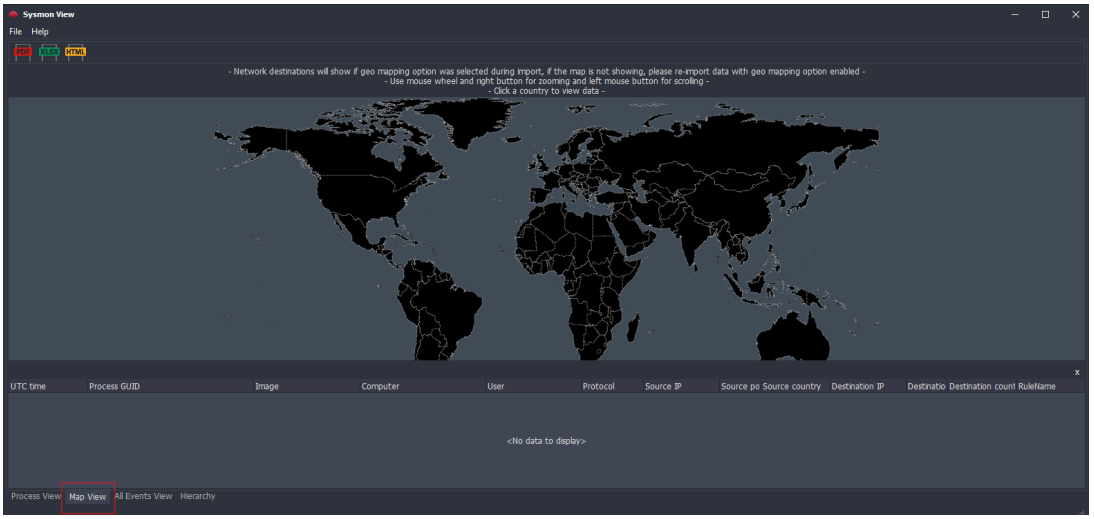
3. Abro el software e importo lo que se guardó anteriormente



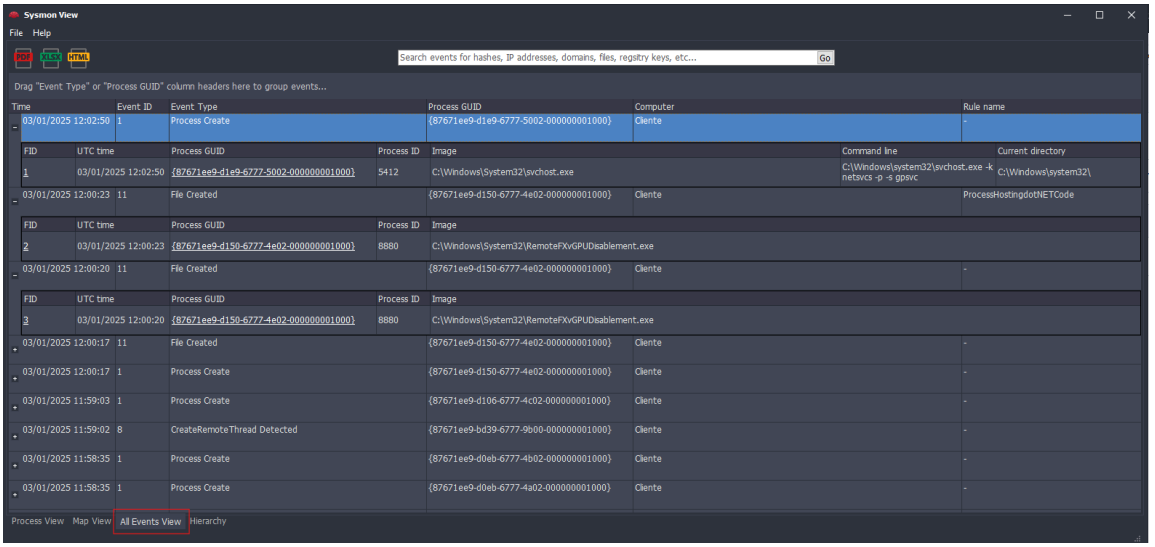
4. La interfaz de Sysmon View está diseñada para analizar y presentar de forma gráfica los eventos registrados por Sysmon.
5. Hay diferentes pestañas que nos muestra información como son:
    a. **Process View:** Muestra una representación visual de los procesos y sus relaciones.
    Qué puedes hacer aquí: Analizar cómo se crean y terminan procesos, Ver qué procesos están vinculados entre sí, Investigar procesos desconocidos o sospechosos.



    b. **Map View:** Proporciona una vista gráfica en forma de mapa de los eventos y las interacciones.
    Qué puedes hacer aquí: Visualizar eventos relacionados, como conexiones de red o modificaciones en el registro, Ver cómo interactúan los procesos con otros recursos del sistema (DNS, archivos, etc.), Identificar patrones en eventos complejos.



c. **All Events View:** Lista todos los eventos registrados de manera detallada.
Qué puedes hacer aquí: Examinar cada evento registrado por Sysmon con detalles como fecha, hora, tipo de evento e ID, Filtrar eventos según ID, procesos o cualquier campo relevante, Usar esta vista para realizar un análisis más detallado.



d. **Hierarchy:** Presenta los eventos en una jerarquía organizada.
Qué puedes hacer aquí: Analizar las relaciones entre eventos, procesos y recursos, Identificar dependencias, como qué proceso generó qué evento, Seguir el flujo lógico de actividades dentro del sistema.