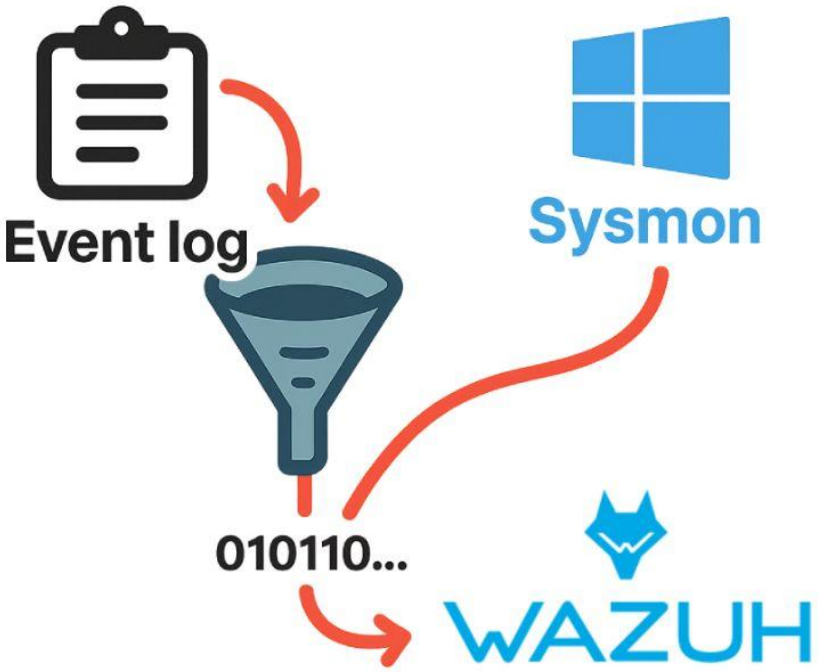
INTEGRACIÓN DE SYSMON EN WAZUH

DETECCIÓN AVANZADA DE AMENAZAS EN WINDOWS

GUÍA



HENRIQUE ALVES

Tabla de contenido

Guía de Configuración de Sysmon y Wazuh para Windows

El procedimiento completo para **configurar Sysmon con Wazuh** se encuentra detalladamente documentado en mi **repositorio de GitHub**. Este repositorio incluye una **guía paso a paso** para implementar reglas personalizadas en **Wazuh**, las cuales permiten mejorar la detección de amenazas y actividades sospechosas en sistemas Windows. Pueden acceder a la guía completa en el siguiente enlace de mi GitHub: Guía de configuración de reglas en Wazuh.

Sysmon, una herramienta avanzada de Microsoft de la suite **Sysinternals**, se utiliza para recopilar registros detallados de actividades del sistema, como la ejecución de procesos, cambios en archivos y conexiones de red. Al integrarse con **Wazuh**, esta herramienta mejora notablemente la capacidad para detectar comportamientos maliciosos o no autorizados en el sistema.

En el proyecto, se configuraron **reglas personalizadas** en **Wazuh** para monitorear eventos específicos generados por **Sysmon**, como la ejecución de procesos no autorizados y la modificación de configuraciones críticas. Estas reglas se diseñaron para optimizar el análisis de eventos y garantizar una respuesta rápida ante posibles incidentes de seguridad.

El resultado de esta configuración es una **mejora significativa** en la visibilidad sobre las actividades del sistema, facilitando la **detección temprana** de amenazas y la capacidad de responder rápidamente a incidentes. Esta integración no solo mejora la detección de eventos, sino que también optimiza el análisis y la gestión de los mismos, mejorando la seguridad general del sistema.

En resumen, la configuración de **Sysmon** con **Wazuh** es una solución poderosa para mejorar la seguridad en sistemas Windows, proporcionando una **detección avanzada** de amenazas, **visibilidad** sobre eventos críticos y una **respuesta eficiente** ante incidentes.

Objetivo del proyecto

El objetivo de este proyecto es integrar Sysmon con Wazuh para crear reglas personalizadas que permitan una mejor detección de amenazas y actividades sospechosas en sistemas Windows. Esta integración facilita la visibilidad de eventos de seguridad, optimizando el análisis y la respuesta ante incidentes en tiempo real.

Los objetivos específicos de este proyecto son:

- Implementar reglas personalizadas en Wazuh para detectar eventos específicos generados por Sysmon.
- Mejorar la visibilidad de las actividades del sistema y las amenazas potenciales.
- Establecer un proceso de respuesta rápida ante incidentes de seguridad.
- Optimizar la gestión de eventos mediante la segmentación por grupos en Wazuh (ej. sistemas Windows y Linux).

Resultados obtenidos

Después de completar la configuración de Sysmon en conjunto con Wazuh, se han obtenido varios resultados clave que mejoran significativamente la capacidad de detección y respuesta ante amenazas en sistemas Windows. A continuación, se destacan los resultados más importantes:

Mejora de la visibilidad en tiempo real:
La integración de **Sysmon** con **Wazuh** ha proporcionado una visibilidad mucho más detallada y en tiempo real de los eventos del sistema. Sysmon recopila información avanzada sobre procesos, conexiones de red, modificaciones en archivos y registros del sistema, mientras que Wazuh procesa esta información para identificar patrones sospechosos. Esto permite una vigilancia más exhaustiva de las actividades dentro del sistema y facilita la detección temprana de posibles amenazas.

Detección precisa de actividades sospechosas:
Las reglas personalizadas implementadas en **Wazuh** permiten detectar eventos específicos generados por Sysmon, como la ejecución de procesos no autorizados, cambios en archivos críticos o alteraciones en configuraciones del sistema. Al identificar comportamientos inusuales o maliciosos de manera rápida y precisa, se mejora significativamente la capacidad para mitigar posibles riesgos antes de que se conviertan en amenazas graves.

Generación de alertas en tiempo real:
Un resultado clave de la integración es la capacidad de generar alertas en tiempo real. Cuando se detecta una actividad sospechosa, **Wazuh** puede generar alertas inmediatamente, lo que permite a los equipos de seguridad actuar rápidamente. Esto no solo mejora la capacidad de respuesta ante incidentes, sino que también ayuda a reducir el impacto de un ataque, minimizando el tiempo de exposición al riesgo.

Optimización del análisis de eventos:
La segmentación de eventos por grupos, como por ejemplo los dispositivos **Windows**, ha permitido una gestión más eficiente de los registros y alertas. Wazuh puede filtrar y priorizar eventos según su relevancia, lo que facilita un análisis más rápido y enfocado. Esto ayuda a los equipos de seguridad a gestionar grandes volúmenes de datos sin perder visibilidad de eventos críticos.

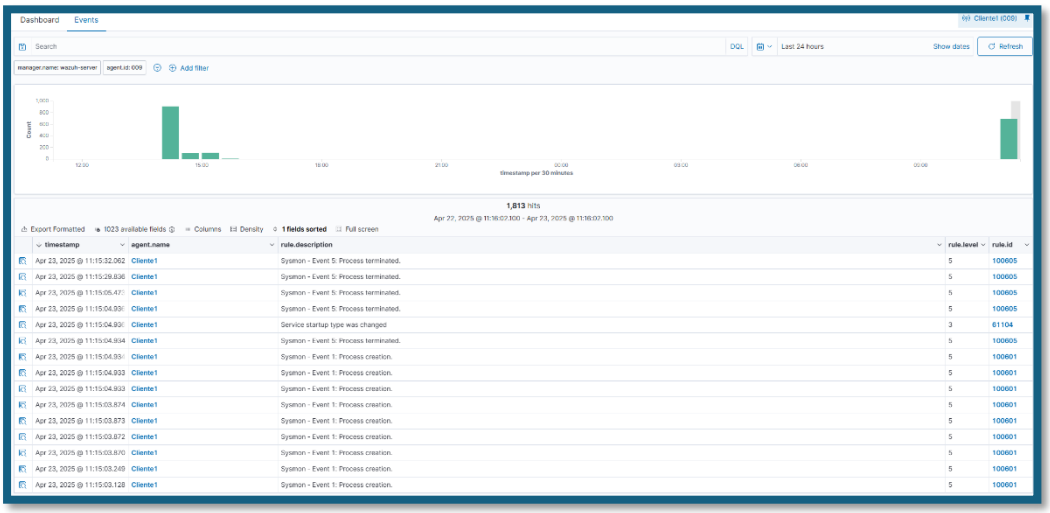
Resultados obtenidos en el Dashboard de Wazuh

La imagen muestra el **dashboard de Wazuh**, donde se visualizan los eventos generados por el agente **Cliente1**. En el gráfico, se observa un pico en la cantidad de eventos alrededor de las **11:15 AM**, lo que indica un aumento en la actividad en ese período.

En la tabla de eventos, se detallan las actividades detectadas por las reglas personalizadas de **Sysmon** en Wazuh, como:

- **Sysmon - Event 5: Process terminated**: Este evento indica que un proceso fue terminado en el sistema.
- **Service startup type was changed**: Este evento alerta sobre un cambio en el tipo de inicio de un servicio, lo que podría ser indicativo de un intento de modificación en los servicios del sistema.
- **Sysmon - Event 1: Process creation**: Este evento registra la creación de nuevos procesos, lo cual es crítico para identificar procesos no autorizados.

Cada evento tiene una marca de tiempo precisa y está asociado con un nivel de severidad (**rule.level**), lo que permite priorizar los eventos según su criticidad. Estos resultados demuestran cómo la integración de Sysmon con Wazuh mejora la visibilidad, facilita la detección de actividades sospechosas y optimiza la respuesta ante incidentes en tiempo real.



Explicación del Evento Registrado en Wazuh

En la imagen se presenta un evento generado por el agente **Cliente1**, donde se registra la ejecución de un proceso en el sistema monitorizado. Este evento se captura a través de la integración de **Sysmon** con **Wazuh**, que permite detectar y registrar eventos detallados relacionados con la ejecución de aplicaciones y procesos en el sistema.

El evento describe la ejecución de un proceso de **Microsoft Edge WebView2**, específicamente el archivo msedgewebview2.exe. Este ejecutable se encuentra en la ruta C:\Program Files (x86)\Microsoft\EdgeWebView\Application\134.0.3124.72\msedgewebview2.exe, lo que indica que se trata de una aplicación legítima utilizada para incrustar contenido web en otras aplicaciones de escritorio.

Hash del Archivo (SHA256)

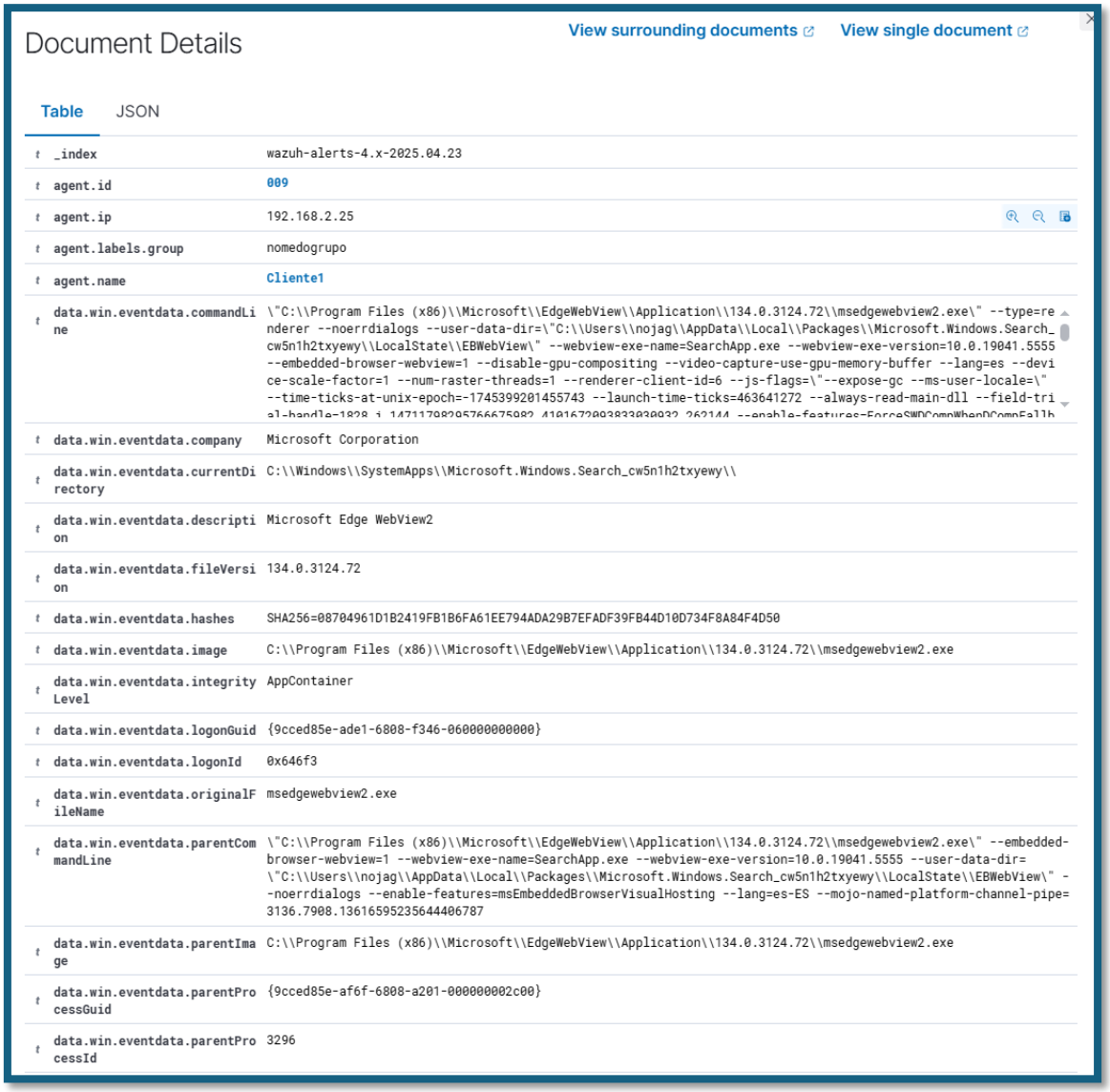
Un dato crucial en este evento es el valor del hash **SHA256**, que se presenta como 08f749601D812419F81B6FA16E749AD429B7EAFD39F84D1D0734F8A84F4D50. Este hash es único para el archivo y se utiliza para verificar su integridad. Un hash permite asegurar que el archivo no ha sido alterado y que su origen es confiable. En un análisis forense, comparar este hash con bases de datos de archivos conocidos permite determinar si el archivo es legítimo o si ha sido comprometido.

Proceso y Jerarquía

La información proporcionada también incluye detalles sobre el **proceso padre** que originó este evento. El **parentProcGuid** y el **parentId** indican el proceso que inició msedgewebview2.exe, permitiendo a los analistas rastrear la cadena de ejecución de los procesos. Esto es útil para detectar procesos sospechosos que podrían haber sido iniciados por aplicaciones maliciosas.

Nivel de Integridad y Seguridad

El evento también indica que el proceso se ejecutó con un **nivel de integridad** de **AppContainer**, lo que significa que se trata de un proceso que tiene restricciones de seguridad. Este tipo de nivel de integridad ayuda a proteger el sistema al limitar lo que el proceso puede hacer, evitando modificaciones críticas del sistema si se trata de un comportamiento no autorizado.



Conclusión

La integración de **Sysmon** con **Wazuh** ha demostrado ser una herramienta poderosa para la detección de amenazas y el monitoreo de eventos en sistemas Windows. En este caso específico, la captura de eventos relacionados con la ejecución de procesos, como el de **Microsoft Edge WebView2**, permite una visibilidad detallada de las actividades del sistema, mejorando significativamente la capacidad de respuesta ante incidentes de seguridad.

El uso de **valores de hash** como el **SHA256** proporciona una capa adicional de seguridad, permitiendo verificar la integridad de los archivos ejecutados y detectar posibles manipulaciones o archivos maliciosos. Además, la capacidad de rastrear la **jerarquía de procesos** a través del **ID del proceso padre** y otros metadatos facilita la identificación de ataques avanzados y comportamientos sospechosos.

Este enfoque no solo mejora la detección de amenazas, sino que también permite **expandir las capacidades de monitoreo**. Con las reglas personalizadas de Wazuh y la integración de Sysmon, es posible detectar una amplia gama de actividades sospechosas, como la creación de procesos no autorizados, cambios en servicios críticos y la ejecución de archivos no verificados. Además, la capacidad de personalizar las reglas permite adaptar la detección a las necesidades específicas de cada entorno, garantizando una protección más robusta y una respuesta más rápida ante incidentes de seguridad.