**Descripción general de Suricata**

Hasta ahora, aprendiste sobre las firmas de detección y conociste Suricata, un sistema de detección de incidentes (IDS).

En esta lectura, aprenderás más sobre Suricata. También descubrirás las ventajas de escribir firmas y configuraciones personalizadas. Esta es una habilidad importante que deberías desarrollar en tu carrera en ciberseguridad, ya que es posible que una de tus tareas sea implementar herramientas IDS y darles mantenimiento.

**Introducción a Suricata**

[**Suricata**](https://suricata.io/) es un sistema de detección de intrusiones de código abierto, un sistema de prevención de intrusiones y una herramienta de análisis de redes.

**Características de Suricata**

Suricata tiene tres funcionalidades principales:

* **Sistema de detección de intrusiones** (**IDS**): Como IDS basado en la red, Suricata puede monitorear el tráfico de la red y alertar sobre intrusiones y actividades sospechosas. Además, se puede configurar como IDS basado en host para que controle el sistema y las actividades de red de un solo host, como una computadora.
* **Sistema de prevención de intrusiones** (**IPS**): Suricata también puede funcionar como un sistema de prevención de intrusiones (IPS) para detectar y bloquear la actividad y el tráfico malicioso. Ejecutar Suricata en modo IPS requiere una configuración adicional, como habilitar el modo IPS.
* **Monitoreo de seguridad de red** (**NSM**):En este modo, Suricata ayuda a mantener la seguridad de las redes al generar y guardar registros de red relevantes. Además, puede analizar el tráfico de red en vivo y los archivos de captura de paquetes existentes, así como crear y guardar capturas de paquetes completas o condicionales. Esto puede ser útil para análisis forenses, respuesta a incidentes y para probar firmas. Por ejemplo, puedes activar una alerta y capturar el tráfico de red en vivo para generar registros de tráfico que luego puedes analizar para refinar las firmas de detección.

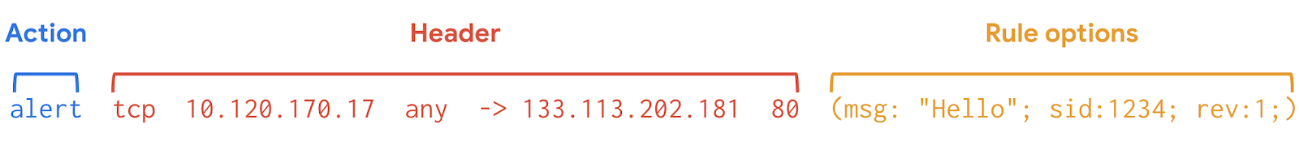
**Reglas**

Las reglas o firmas se utilizan para identificar patrones, condiciones y  comportamientos específicos del tráfico de red que podrían indicar actividad maliciosa. En Suricata, los términos regla y firma suelen ser intercambiables. Los analistas de seguridad utilizan **firmas** o patrones asociados con actividades maliciosas para detectar y alertar sobre amenazas específicas. Las reglas también se pueden usar para proporcionar mayor contexto y visibilidad en sistemas y redes, lo que contribuye a identificar posibles amenazas o vulnerabilidades de seguridad.

Suricata utiliza el **análisis de firmas**,que es un método de detección utilizado para encontrar eventos de interés. Las firmas tienen tres componentes:

* **Acción**: El primer componente de una firma. Describe qué hay que hacer si la actividad de la red o del sistema coincide con la firma, por ejemplo, alertar, pasar, soltar o rechazar.
* **Encabezado**: Incluye información de tráfico de red, como direcciones IP de origen y destino, puertos de origen y destino, protocolo y dirección de tráfico.
* **Opciones de regla:** Proveen diferentes opciones para personalizar las firmas.

Este es un ejemplo de una firma de Suricata:



Las opciones de regla tienen un orden específico, y cambiarlo modificaría el significado de la regla.

**Nota**: Los términos regla y firma son sinónimos.

**Nota:** El orden de  reglas hace referencia al orden en que Suricata las evalúa. Las reglas se procesan en el orden en que están definidas en el archivo de configuración. Sin embargo, Suricata procesa las reglas en un orden predeterminado diferente: pass, drop, reject y alert (pasar, soltar, rechazar y alertar). El orden de las reglas afecta el veredicto final de un paquete. Por ejemplo, si las reglas con acciones en conflicto, como una regla de soltar y una regla de alertar, coinciden en el mismo paquete.

**Reglas personalizadas**

Aunque Suricata ya tiene reglas previamente escritas, es muy recomendable modificarlas o personalizarlas para que cumplan con los requisitos de seguridad específicos.

No hay un único enfoque para la creación y modificación de las reglas y esto se debe a que la infraestructura de TI de cada organización es diferente. Los equipos de seguridad deben probar y modificar exhaustivamente las firmas de detección de acuerdo a sus necesidades.

La creación de reglas personalizadas ayuda a personalizar la detección y el monitoreo. Además, contribuye a minimizar la cantidad de falsos positivos que los equipos de seguridad reciben. Saber cómo escribir firmas efectivas y personalizadas es muy importante para aprovechar al máximo las tecnologías de detección.

**Archivo de configuración**

Antes de implementar las herramientas de detección y que comiencen a monitorear sistemas y redes, es necesario configurar correctamente los ajustes, para que hagan la tarea que se necesita. Esto se hace por medio del **archivo de configuración**, que permite configurar los ajustes de una aplicación y personalizarla. De esta manera, se indica exactamente cómo se desea que los IDS interactúen con el resto del entorno.

En Suricata, el archivo de configuración es **suricata.yaml**, que utiliza el formato de archivo YAML para la sintaxis y la estructura.

**Archivos de registro**

Cuando se activan las alertas, Suricata genera dos archivos de registro:

* **eve.json**: es el archivo de registro estándar de Suricata y contiene información detallada y metadatos sobre los eventos y alertas generados por Suricata, almacenados en formato JSON. Por ejemplo, los eventos en este archivo contienen un identificador único llamado flow\_id, que se utiliza para correlacionar registros o alertas con un solo flujo de red, lo que facilita el análisis del tráfico de red. El archivo eve.json se utiliza para hacer un análisis más detallado, y se considera un mejor formato de archivo para el análisis sintáctico de registros y la ingestión de registros SIEM.
* **fast.log**: Se utiliza para registrar información de alerta mínima, incluida la dirección IP básica y los detalles de puerto sobre el tráfico de la red. Además, es útil para generar registros y alertas básicos, y se considera un formato de archivo heredado que no es adecuado para la respuesta a incidentes o tareas de caza de amenazas.

La principal diferencia entre ambos es el nivel de detalle que se registra en cada uno. El archivo fast.log registra información básica, mientras que el archivo eve.json contiene información detallada adicional.

**Conclusiones clave**

En esta lectura, exploraste algunas de las características de Suricata, su sintaxis de reglas y la importancia de su configuración. Comprender cómo configurar las tecnologías de detección y escribir reglas efectivas te dará una visión clara de la actividad que ocurre en un entorno, para que puedas mejorar la capacidad de detección y la visibilidad de la red. Podrás comenzar a practicar con Suricata en la próxima actividad.

**Recursos para obtener más información**

Si deseas obtener más información sobre Suricata, incluida la gestión y el rendimiento de las reglas, puedes consultar los siguientes recursos:

* [Guía de usuario de Suricata](https://suricata.readthedocs.io/en/latest/index.html)
* [Características de Suricata](https://suricata.io/features/)
* [Gestión de reglas](https://suricata.readthedocs.io/en/latest/rule-management/suricata-update.html.html)
* [Análisis del desempeño de las reglas](https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html#engine-analysis-and-profiling)
* [Webinario de caza de amenazas de Suricata](https://youtu.be/kaDGolhTu94)
* [Introducción a la creación de reglas en Suricata](https://youtu.be/tvoqFBVSShA)
* [Ejemplos de jq de eve.json](https://suricata.readthedocs.io/en/latest/output/eve/eve-json-examplesjq.html)

Marcar como completo

Me gusta

No me gusta

Informar de un problema