Análisis de SIEM

Sergio Rosello Morell

En el presente documento, se van a analizar cinco soluciones SIEM Open-Source y cinco soluciones SIEM Comerciales. Este análisis se va a centrar en proporcionar una opinión informada al lector para que pueda responder a una serie de preguntas clave que debe hacerse cuando la organización se plantea implementar un SIEM.

- Como de bien se adapta el SIEM a las tecnologías que usa mi organización
- Que necesita mi organización
- Cuanto dinero puede gastar mi organización en la solución SIEM
- Flexibilidad de la plataforma

SIEM Open Source

A continuación se listan las 5 soluciones SIEM Open Source.

1. Apache Metron

Es una evolución del proyecto Cisco OpenSOC, desarrollado con la intención de <++> y evolucionado por la comunidad de Hadoop para convertirlo en lo que es ahora.

En Septiembre de 2014, Cisco anuncia la plataforma Cisco OpenSOC para posteriormente dejar de darle soporte, pero gracias a la comunidad de desarrolladores que usaban el servicio, siguió evolucionando, hasta que en Diciembre del 2015, la fundación Apache acepta el rol de mantener el proyecto y trabaja para ampliar los casos de uso para el mismo, añadiendo soporte para muchas mas aplicaciones, firewalls, sistemas Intrusion Detection y mas.

OpenSOC fue el primer proyecto que usa en combinación Storm, Hadoop y Kafka, cambiando el paradigma de aplicación monolito a aplicación integrada, que une varios proyectos Open Source.

Metron esta formada por cuatro capacidades:

- Almacenamiento de registros (Almacenamiento ligero, seguro y con capacidades de búsqueda rápida de eventos pasados)
- Módulos (Para analizar distintas fuentes de información, como pcap, netflow, bro, snort fireye, ademas de la posibilidad de crear una que se ajuste a las necesidades de la empresa.)
- Aplicación de seguridad (Proporciona funcionalidades SIEM, como alertas, eventos, gráficos)
- Detección de anomalías (Uso de algoritmos *Machine Learning* para analizar el flujo de datos en tiempo real.)

Todas estas partes unidas, hacen de Metron una solución SIEM muy valida y modular.

Los usuarios que van a usar Metron son:

- Analista SOC
- Investigador SOC
- Director SOC
- Investigador Forense
- Investigador de ciberseguridad de la plataforma
- *Data Scientist* de seguridad

Las ventajas de Metron son:

- Proporciona la capacidad de gestionar y analizar alertas
- Almacena datos contextuales (Bueno para analizar eventos de seguridad pasados)
- Investigación (Proporciona herramientas para la investigación de vulnerabilidades e intrusiones)

2. AlienVault OSSIM

Creado por AT&T, este SIEM, que sigue en desarrollo, es la parte gratuita del servicio que ofrecen con su SIEM mas completo y comercial: USM Anywhare. Las características de este SIEM lo hacen ideal para empresas pequeñas y medianas, ya que cuando la organización crece y necesita mas recursos y por tanto, un SIEM mas potente, este no esta a la altura. Ademas, AlienVault no esta disponible para entornos basados en la nube y solo puede correr en un servidor, haciendo de el, un SIEM con fecha de caducidad, si la empresa tiene previsto crecer próximamente o cambiar su estrategia tecnológica a la nube.

En la propia pagina web de la solución de software libre, aparece la comparativa con su solución comercial. Ademas, parece que esta solución es una buena herramienta para el análisis en tiempo real de los datos. Cualquier otro tipo de requisito por parte de los operadores del SIEM, quedara escaso. Por ejemplo, el tiempo medio en el que se encuentra una vulnerabilidad en el sistema es de 8 meses, pero esta herramienta no funciona correctamente cuando los registros superan los 6 meses. Ademas, las capacidades de búsqueda en la propia base de datos son limitadas.

3. MozDef

Este proyecto nace como respuesta a la creciente disponibilidad de herramientas de automatización y coordinación de las que disponen los Hackers para infiltrarse en una organización.

La finalidad de esta plataforma es:

- Proporcionar una plataforma para que los analistas de seguridad puedan detectar rápidamente un incidente de seguridad.
- Automatizar interfaces a otros sistemas con API, para agilizar el proceso de detección de amenazas.

- Proporcionar métricas de incidentes y eventos
- Facilitar la colaboración en tiempo real entre los analistas
- Facilitar la estandarización del proceso de análisis de incidentes

Para ello, se ha centrado mucho en ser modular, proporcionando distintos puntos a lo largo del flujo de datos en los que se pueden alterar los datos con scripts de Python, para adaptarlos a las entradas esperadas, ademas de analizar los datos de forma mas profunda, haciendo uso de herramientas de aprendizaje automático o enriquecimiento de datos, entre otras soluciones.

Ademas de gestionar y almacenar los eventos de seguridad, también es necesario que un buen SIEM proporcione a la organización la posibilidad de gestionar los incidentes de forma correcta. MozDef usa Meter por debajo, que es un protocolo para enviar información a través de la red de forma "raw". Esto quiere decir, que los analistas de seguridad que estén usando MozDef van a poder ver los registros, incidentes y acciones en tiempo real.

4. Wazuh

Este proyecto salio de OSSEC, un SIEM que entro en fase de mantenimiento en 2015. Entonces, el equipo de Wazuh decidió montar esta solución con la base del proyecto OSSEC.

La ventaja de esta decisión, es que el equipo se ha podido centrar en implementar características que quería la comunidad de OSSEC, y no en montar un SIEM desde cero, para posteriormente añadir las características que solicitaba la comunidad. Ademas de esta decisión, han añadido la opción de usar Wazuh en la nube, aunque el equipo que quiera usarlo en la nube, deberá pagar 500 euros al mes para la solución mas barata.

5. Security Onion

Security Onion nos proporciona una distribución de GNU/Linux completa diseñada específicamente para la búsqueda activa de amenazas, monitorización de seguridad y gestión de registros.

Una de las características mas importantes, es que une registro de paquetes de red, detección de red y endpoint (Alertas, metadata, monitorización, registros, etc...) y una buena herramienta de análisis, en la Security Onion Console.

Une distintos proyectos Open Source para crear la plataforma, como Google Steganogrpher, Elasticsearch, Logstash, Kibana, Suricata entre otros.

Como cualquier otro SIEM moderno, Security Onion tiene incorporado en el SIEM una herramienta llamada "TheHive" para gestionar los eventos que van apareciendo en la red. De esta forma, distintos miembros del equipo de analistas de la red están informados sobre el estado de las diferentes alertas en tiempo real.

SIEM Comerciales

A continuación se listan las 5 soluciones SIEM Comerciales.

1. **Empow**
2. **IBM QRadar**
3. **Lacework**
4. **Logryth**
5. **Splunk**

Conclusión