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 responder a algunas preguntar clave, que debe hacer cualquier organización cuando esta planteando implementar una solución 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

3. MozDef

4. Wazuh

5. Security Onion

SIEM Comerciales

A continuación se listan las 5 soluciones SIEM Comerciales.

1. Empow

2. IBM QRadar

3. Lacework

4. Logryth

5. Splunk

Conclusión