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.

SIEM Open Source

A continuación se listan las 5 soluciones SIEM Open Source.

1. Apache Metron

Es una evolución del proyecto Cisco OpenSOC, 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

Esta herramienta, nos proporciona una buena forma de gestionar la seguridad de una empresa mediana o pequeñas de forma semi-automática.

Este SIEM esta diseñado para empresas con poder adquisitivo significativo, que si que les importa la seguridad. Posiblemente porque deben cumplir una certificación, legislación o reconocimiento de una entidad externa.

Se centran en que un solo analista de seguridad puede gestionar toda la parte de administración y gestión de la seguridad de la empresa con su producto. Esto es posible porque se automatiza el proceso de una forma que proporciona al analista la mayoría de herramientas que necesita para gestionar la seguridad de la empresa. Como inconveniente, el mismo analista no tiene tanta flexibilidad a la hora de gestionar eventos no definidos en el sistema que viene ya reinstalado. Esto implica que el analista, tampoco tiene un nivel de conocimiento muy extenso, ya que de otra forma, posiblemente prefiera tener el control de las tecnologías en uso, ademas de los eventos a monitorizar.

La tecnología que usa la empresa Empow, esta basada en Inteligencia Artificial como pieza clave del proceso de monitorización. Empow define a su solución SIEM como el único SIEM de nueva generación. Justamente porque usa inteligencia artificial para gestionar, analizar, predecir y agrupar los ataques que recibe la red empresarial.

2. IBM QRadar

Proporciona a los analistas y sus responsables la capacidad de gestionar eventos de seguridad. Ademas, interrelaciona varias evidencias en posibles eventos únicos, como por ejemplo, agrupa varios intentos de inicio de sesión desde la misma IP como un único ataque, en vez de mostrar cada evento como una ocurrencia aislada.

Esta herramienta esta diseñada para empresas mas grandes que Empow, con equipo enteros dedicados al análisis de la red sobre la que esta montado el SIEM.

Por lo general, la decisión de la adquisición de la tecnología no depende del analista mas experimentado o del responsable de seguridad de la empresa, sino posiblemente venga de una decisión no informada de un rol de gestión.

Este SIEM proporciona al analista la capacidad de gestionar la red directamente desde la consola. Es una plataforma muy sencilla de operar y muy completa.

Proporciona mucho control a los analistas y estos no tienen por que ser analistas experimentados para poder gestionar la seguridad de la red de forma determinante para su propia seguridad.

Análisis de usuarios basado en desviación de la norma. Es decir, determina en riesgo de los usuarios dependiendo de las acciones que realizan estos mismos.

Para poder usar el SIEM en su máximo esplendor, el SIEM depende de tecnología como IBM Watson, o IBM X-Force. Ambos servicios hacen que la empresa se adentre mas y mas en el ecosistema de IBM.

3. Lacework

Bajo primera apariencia, la empresa que ha creado este SIEM no tiene la liquidez económica para dedicar a la parte de ventas del producto, seguramente porque se centren mas en calidad que en ventas. Esto es indicativo de una empresa en crecimiento y en plena fase de construcción de su producto.

Parece que el sistema se centra en la calidad de su producto, mas que el las ventas, a diferencia de los otros SIEM.

Este SIEM esta dedicado a la nueva generación de analistas, un tanto híbridos entre el mundo de la seguridad como en el mundo de DevOps.

La faceta mas importante de este SIEM es que esta destinado a una infraestructura en la nube. A medida que las tecnología Cloud van aumentando y las empresas van transición ando de equipos locales a equipos y estructuras en la nube, este tipo de SIEM es una señal de madurez, tanto de las tecnologías Cloud, como de el mismo SIEM, ya que es uno de los pioneros en implementar esta funcionalidad.

Esta plataforma se centra en proporcionar al analista un estado de la red, para que posteriormente el analista pueda realizar comprobaciones basándose en el estado de la red.

Esto requiere un analista mucho mas capaz y hábil que otras soluciones SIEM, como IBM QRadar, en las que el analista prácticamente puede operar y detectar amenazas en la red con un curso de formación de algunas semanas, sin conocimiento previo de ciberseguridad.

La forma que tiene Lacework de avisar al analista de seguridad que algo ha pasado se basa en un IDS con aprendizaje automático. Este sistema revisa el uso de las maquinas en la red de forma constante y si existe algún evento fuera de lo normal, avisa al analista con la información, gradualmente granular y completa.

Parece un SIEM dedicado a analistas de seguridad con mucho conocimiento sobre su propia arquitectura de red, ademas, de mucho conocimiento de que debería correr que maquina en que momento. Esto es posible para empresas pequeñas y medianas, ya que para las empresas grandes, tanto la interfaz gráfica como los requisitos sobre el conocimiento del analista son demasiado restrictivos para que funcione correctamente.

4. Logrhyth

Esta empresa ha conseguido ser incluida 8 veces en el reporte de Gartner en el cuadrante mágico. Con su solución SIEM para entornos Cloud, es la competencia directa de Lacework.

Esta solución esta entre el SIEM proporcionado por IBM y Lacework, en cuanto a madurez de la interfaz gráfica y posibilidades en cuanto a análisis de vulnerabilidades y seguimiento de un incidente.

La interfaz gráfica permite al analista seguir una serie de pasos especificados, llamados "Playbooks", que aseguran al analista no perder el hilo de la investigación del incidente.

La capacidad de investigación del analista debe ser mas alta que la de un analista de una plataforma como la de IBM, pero mas baja que la de Lacework. Esto se debe a que el analista debe saber que buscar, pero existen sitios en los que analizar y registrar los eventos encontrados. Ademas, es importante que el analista sepa usar comandos como "whois" y para que sirven, porque, aunque la herramienta proporciona una abstracción a ella, se sigue teniendo que ejecutar bajo petición.

La interfaz gráfica proporciona la capacidad de gestionar un único incidente entre uno o mas analistas a tiempo real. Esto significa que, en caso de un incidente, el equipo tiene en la misma plataforma la capacidad de: Seguir un "Playbook" predefinido, para no perder ningún detalle y mantener siempre la perspectiva en el caso. Asignar a cada miembro del equipo a una tarea específica del "Playbook". Mantener un sitio centralizado en el que poder ver las pruebas y construir teorías del incidente. Y proporciona toda la información necesaria, o la capacidad de generar la información necesaria en cada momento de la fase de investigación.

5. Splunk

Esta solución SIEM proporciona al analista una visualización muy detallada de todos los eventos que existen en el sistema. Ademas, proporciona al analista una serie de utensilios, como la visualización de una incidencia desglosada en espacio temporal para poder darle sentido a los hechos muy completa.

Esta herramienta proporciona la capacidad de analizar cualquier evento, desde distintos productos, con distintos tipos de registros de una forma sencilla, gracias a la comunidad que ha conseguido crear Splunk. Si tienes una tecnología que quieres monitorizar, seguramente ya haya sido creada la regla de parseado para ella.

La mayor ventaja de Splunk es la granularidad y capacidad de investigación que proporciona al analista de los registros ingeridos. Como consecuencia, el analista debe ser una persona formada en el ámbito de la ciberseguridad.

Conclusión

Todos los SIEM analizados existen en un mercado aparentemente plagado de posibilidades, en el que los responsables de la decisión de SIEM deben tener una serie de cosas muy claras. Estas cosas son:

1. Capacidad de monitorización en tiempo real
2. Respuesta a incidentes
3. Monitorización de usuarios
4. Análisis de amenazas
5. Analíticas avanzadas en base a los registros originales
6. Detección de amenazas avanzado
7. Buena gestión de registros
8. Escalabilidad

Cumplir todos estos requisitos, es, de por si un requisito muy complicado de conseguir, por tanto, el responsable de la decisión, deberá revisar cada una de las tecnologías planteadas en el informe redactado para la correcta decisión.

En cuanto a la diferencia entre SIEM comerciales y SIEM Open Source, es bastante grande. Por lo general, los SIEM Open Source proporcionan a la organización una modularidad sin limites, pero a medida que la organización va creciendo, es probable que deba generar nuevos módulos que se adapten a sus requisitos. Los SIEM comerciales proporcionan la facilidad y funcionalidad de un producto completo, concebido desde arriba a abajo para realizar la función que se espera, por tanto, el rendimiento en esa misma función y caso de uso, debe ser muy optima y pulida, pero el rendimiento en áreas en las que no se ha definido un caso de uso o simplemente, se necesita una forma distinta de gestionar la incidencia, pueden ser mucho mas complejas de gestionar ya que la organización no depende del talento de sus trabajadores en generar la solución, sino que depende de la empresa a la que le ha comprado la solución.

En mi opinión, se puede crear un SIEM Open Source completamente valido desde el punto de vista de la ciberseguridad si existe una buena política de seguridad en la empresa y los lideres están concienciados por la seguridad. A medida que esta empresa vaya creciendo, también lo hará el SIEM, porque pasa a ser un producto de la misma empresa, o del equipo que se encarga de la seguridad de la organización.

Para empresas en las que la seguridad no es primera preocupación, seguramente no usen un SIEM desde su concepción, y por tanto, cuando pasen a necesitarlo, sea demasiado tarde para usar un SIEM Open Source, por el nivel de cambios, mejoras, adaptaciones que se deben hacer para llegar al nivel de madurez del SIEM que necesita en el estado en el que se encuentra la empresa.