11 HERRAMIENTAS SIEM DE CÓDIGO ABIERTO

Los sistemas SIEM se están convirtiendo en la piedra angular de los paradigmas de seguridad implantados por un número cada vez mayor de organizaciones, ya que ayudan a proteger los entornos informáticos de los ciberataques y a cumplir con las cada vez más estrictas normas de conformidad.

En un artículo anterior, explicamos qué es realmente un sistema SIEM: por qué las organizaciones lo necesitan para empezar, los componentes que lo componen y cómo ayuda a mitigar los ataques. Una de las conclusiones a las que se llegó en ese artículo fue que SIEM no es en realidad una única herramienta en sí misma, sino que se compone de múltiples componentes de monitorización y análisis.

Existen plataformas propietarias que sí ofrecen una solución SIEM todo en uno, como LogRhythm, QRadar y ArcSight. Estas soluciones pueden resultar bastante caras, sobre todo a largo plazo y en grandes organizaciones, por lo que cada vez más empresas buscan una plataforma SIEM de código abierto.

Pero, ¿existe una plataforma de código abierto que incluya todos los ingredientes SIEM básicos?

Por eso existe Logz.io Cloud SIEM, una recopilación de opciones de código abierto para crear una solución de seguridad de defensa prioritaria para la observabilidad, basada en gran medida en la pila ELK.

No existe un sistema SIEM de código abierto perfecto todo en uno. Las soluciones existentes carecen de las capacidades básicas de SIEM, como la correlación de eventos y la generación de informes, o requieren la combinación con otras herramientas.

1. OSSIM

OSSIM, la versión de código abierto de la oferta de Gestión Unificada de la Seguridad (USM) de AlienVault, es probablemente una de las plataformas SIEM de código abierto más populares. OSSIM incluye componentes SIEM clave, a saber, recopilación, procesamiento y normalización de eventos y, lo que es más importante, correlación de eventos.

OSSIM combina las capacidades nativas de almacenamiento y correlación de registros con numerosos proyectos de código abierto para construir un SIEM completo. La lista de proyectos de código abierto incluidos en OSSIM incluye: FProbe, Munin, Nagios, NFSen/NFDump, OpenVAS, OSSEC, PRADS, Snort, Suricata y TCPTrack.

La inclusión de OpenVAS es de particular interés, ya que OpenVAS se utiliza tanto para la evaluación de vulnerabilidades mediante la correlación de los registros de IDS con los resultados del escáner de vulnerabilidades.

Como era de esperar, el OSSIM de código abierto no es tan rico en funciones como su "hermano mayor" comercial. Ambas soluciones funcionan bien para despliegues pequeños, pero los usuarios de OSSIM experimentan importantes problemas de rendimiento a gran escala, lo que en última instancia les hace decantarse por la oferta comercial. Las capacidades de gestión de registros en la versión de código abierto de OSSIM, por ejemplo, son prácticamente inexistentes.

2. LA PILA ELK

La pila ELK es posiblemente la herramienta de código abierto más popular utilizada hoy en día como componente básico de un sistema SIEM. Un componente básico, sí. Un sistema SIEM completo, no, ya que hay mucho espacio para el debate sobre si la pila ELK es o no un sistema SIEM "todo en uno".

La pila ELK está formada por los productos de código abierto Elasticsearch, Logstash, Kibana y la familia Beats de cargadores de registros. Aunque es importante tener en cuenta que Elasticsearch y Kibana estarán bajo licencias SSPL a partir del 14 de enero de 2021.

Logstash es un agregador de registros que puede recopilar y procesar datos de casi cualquier fuente de datos. Puede filtrar, procesar, correlacionar y, en general, mejorar cualquier dato de registro que recopile. **Elasticsearch** es el motor de almacenamiento y una de las mejores soluciones en su campo para almacenar e indexar datos de series temporales. **Kibana** es la capa de visualización de la pila y es extremadamente potente. **Beats** incluye una variedad de cargadores de registros ligeros que se encargan de recopilar los datos y enviarlos a la pila a través de Logstash.

Logstash utiliza una amplia gama de plugins de entrada para recopilar registros. Sin embargo, también puede aceptar entradas de soluciones más específicas como OSSEC o Snort (véase más abajo). Combinadas, las capacidades de procesamiento, almacenamiento y visualización de registros de ELK Stack son funcionalmente inigualables. Sin embargo, a efectos de SIEM, a ELK Stack, al menos en su formato de código abierto, le faltan algunos componentes clave.

En primer lugar, no hay capacidad integrada de generación de informes o alertas. Se trata de un problema conocido no sólo para los usuarios que intentan utilizar la pila para la seguridad, sino también para casos de uso más comunes, como las operaciones de TI. Las alertas pueden añadirse utilizando el X-Pack, un producto comercial de Elastic, o añadiendo complementos de seguridad de código abierto.

Tampoco hay reglas de seguridad integradas que puedan utilizarse. Esto hace que la pila sea un poco más costosa de manejar, tanto en términos de recursos como de costes operativos.

3. OSSEC

OSSEC es un popular Sistema de Detección de Intrusiones en el Host (HIDS) de código abierto que funciona con varios sistemas operativos, incluyendo Linux, Windows, MacOS, Solaris, así como OpenBSD y FreeBSD.

El propio OSSEC se divide en dos componentes principales: el gestor (o servidor), responsable de recopilar los datos de registro de las distintas fuentes de datos, y los agentes, aplicaciones encargadas de recopilar y procesar los registros y facilitar su análisis.

El proyecto OSSEC en sí no incluye una capa de visualización. Existía una interfaz de usuario que fue obviada y, en su lugar, la recomendación es utilizar herramientas de visualización externas como Kibana y Grafana.

OSSEC monitoriza directamente una serie de parámetros en un host. Esto incluye archivos de registro, integridad de archivos, detección de rootkits y monitoreo del registro de Windows. OSSEC puede realizar análisis de registros de otros servicios de red, incluidos la mayoría de los populares FTP de código abierto, correo, DNS, base de datos, web, firewall y soluciones IDS basadas en red. OSSEC también puede analizar registros de una serie de servicios de red y soluciones de seguridad comerciales.

OSSEC dispone de varias opciones de alerta y puede utilizarse como parte de soluciones automatizadas de detección de intrusiones o de respuesta activa. OSSEC tiene un motor de almacenamiento de registros primitivo. Por defecto, los mensajes de registro de los agentes anfitriones no se conservan. Una vez analizados, OSSEC elimina estos registros a menos que se incluya la opción <logall> en el archivo ossec.conf del gestor de OSSEC. Si esta opción está activada, OSSEC almacena los registros entrantes de los agentes en un archivo de texto que se rota diariamente.

Es discutible si OSSEC puede considerarse un sistema SIEM "todo en uno". No cabe duda de que OSSEC hace el trabajo duro que supone implantar un sistema SIEM: recopila datos y los analiza, pero carece de algunos de los componentes básicos de gestión y análisis de registros necesarios. Vale la pena señalar que el proyecto OSSEC ha sido bifurcado por otras soluciones HIDS (por ejemplo, Wazuh) que amplían la funcionalidad de OSSEC y lo convierten en una opción SIEM más completa.

4. WAZUH

Wazuh es una solución HIDS bifurcada de OSSEC. Se describe a sí misma como una "solución de monitorización de seguridad preparada para la empresa" que es totalmente compatible y está dotada tanto de capacidades de respuesta a incidentes como de monitorización de la integridad. Los creadores de Wazuh sostienen que OSSEC no había recibido suficientes actualizaciones antes de 2015, cuando se lanzó Wazuh por primera vez.

Wazuh pretende añadir escalabilidad a OSSEC. Eso incluye soporte para Puppet, Chief, Docket y Ansible. El soporte de clúster y el soporte multihilo, además de las capacidades anti-inundación, controlan un mayor rendimiento para un escalado horizontal sostenible. También se integra con Suricata o el proyecto Owhl para NIDS, otras bases de datos. Dispone de módulos y decodificadores tanto para AWS como para Microsoft Azure. Por el lado de ELK Stack, es totalmente compatible a través del plugin Wazuh Kibana y enriquecimiento de datos a través de un módulo GeoIP Logstash.

Su documentación incluye enlaces a la actualización de servidores y agentes para migrar de OSSEC a Wazuh. A partir de la actualización 3.7.1, se incluye más información de rastreo en los registros del modo de depuración. En 3.7.2, Wazuh corrigió problemas relacionados con su módulo Logcollector, ahora descartando líneas con caracteres binarios.

5. APACHE METRON

Proyecto retirado, desarrollado a partir de la plataforma OpenSOC de Cisco y lanzado por primera vez en 2016, Apache Metron es un actor relativamente nuevo en la industria y otro ejemplo de un marco de seguridad que combina múltiples proyectos de código abierto en una plataforma.

Desde una perspectiva arquitectónica, Metron se basa en otros proyectos de Apache para recopilar, transmitir y procesar datos de seguridad. Las sondas Apache Nifi y Metron recopilan datos de fuentes de datos de seguridad que se introducen en temas separados de Apache Kafka. Posteriormente, los eventos se analizan y normalizan en JSON estándar y, a continuación, se enriquecen y, en algunos casos, se etiquetan. Se pueden activar alertas si se identifican determinados tipos de eventos. Para la visualización, se utiliza Kibana (aunque es una versión obsoleta).

Para el almacenamiento, los eventos se indexan y persisten en Apache Hadoop y Elasticsearch o Solr en función de las preferencias de la organización. Además de estos datos, Metron proporciona una interfaz para centralizar el análisis de los datos con resúmenes de alertas y datos enriquecidos.

Una de las características más destacadas de Metron es su arquitectura ampliable y conectable. Los sensores Bro, pycapa y fastcapa, por ejemplo, pueden utilizarse para enviar datos específicos a Metron. Mediante Stellar, un sencillo DSL, los usuarios pueden escribir sus propias funciones para transformar los datos recopilados. Una extensa API REST permite a los usuarios interactuar con Metron, de modo que pueden, por ejemplo, gestionar alertas mediante programación.

Al ser relativamente joven, Metron aún tiene carencias en algunos aspectos. Metron sólo puede instalarse en un número limitado de sistemas operativos y entornos, aunque admite escenarios de automatización con Ansible e instalación a través de Docker (sólo Mac y Windows). La interfaz de usuario es un poco inmadura y no soporta autenticación, por ejemplo.

6. SIEMONSTER

SIEMonster es otro joven jugador SIEM pero uno extremadamente popular también, con más de 100.000 descargas en sólo dos años. SIEMonster se basa en tecnología de código abierto y está disponible de forma gratuita y como solución de pago (Premium y MSSP multi-tenancy).

Aunque SIEMonster utiliza su propia terminología "monstruosa" para denominar las distintas funciones SIEM del sistema (por ejemplo, Kraken), los componentes subyacentes son tecnologías de código abierto bien conocidas. La pila ELK se utiliza para la recopilación (Filebeat y Logstash), procesamiento, almacenamiento y visualización de los datos de seguridad recopilados. RabbitMQ se utiliza para las colas. SearchGuard se utiliza para el cifrado y la autenticación sobre Elasticsearch y ElastAlert para las alertas. Un fork de OSSEC Wazuh para HIDS. Y la lista continúa.

Desde el punto de vista de la funcionalidad, SIEMonster incluye todos los elementos que un analista podría desear, a los que se accede a través de un menú principal: la interfaz de usuario Kibana para buscar y visualizar datos, una interfaz de usuario MineMeld para inteligencia sobre amenazas y Alerts para crear y gestionar notificaciones basadas en eventos. Otras herramientas de código abierto integradas son DRADIS, OpenAudit y FIR.

SIEMonster puede desplegarse en la nube mediante contenedores Docker, lo que facilita la portabilidad entre sistemas, pero también en máquinas virtuales y en sistemas de metal desnudo (Mac, Ubuntu, CentOS y Debian). La documentación es extensa, aunque se echa en falta una versión en línea.

7. PRELUDE

Similar a OSSIM, Prelude es un marco SIEM que unifica varias otras herramientas de código abierto. Y como OSSIM, también es una versión de código abierto de la herramienta comercial del mismo nombre. Prelude pretende cubrir las funciones que herramientas como OSSEC y Snort dejan fuera.

Prelude acepta registros y eventos de múltiples fuentes y los almacena en una única ubicación utilizando el formato de intercambio de mensajes de detección de intrusiones (IDMEF). Proporciona funciones de filtrado, correlación, alerta, análisis y visualización.

Una vez más, al igual que OSSIM, la versión de código abierto de Prelude es significativamente limitada en comparación con la oferta comercial en todas estas capacidades, que es probablemente la razón por la que no es muy popular. Citando la documentación oficial "Prelude OSS está destinado a evaluación, investigación y pruebas en entornos muy pequeños. Tenga en cuenta que las prestaciones de Prelude OSS son muy inferiores a las de la edición SIEM de Prelude."

8. SECURITYONION

SecurityOnion es una distribución (distro) Linux gratuita para la detección de intrusos y la supervisión de la seguridad en redes (NSM) y empresas (ESM). Se apoya en otros proyectos de código abierto como ELK Stack, OSSEC, Snort (más información a continuación), Suricata y otros. Fue desarrollado por Doug Burks y lanzado en 2008, quien más tarde lanzó Security Onion Solutions en 2014.

Ofrece sistemas de detección de intrusiones (IDS) basados en host y en red, así como captura de paquetes completa (FPC) a través de netsniff-ng para detectar eventos como la filtración de datos, malware, correos electrónicos de phishing y otros exploits en redes (otras opciones de código abierto para FPC incluyen TCPDUMP basado en GUI y la interfaz de línea de comandos Wireshark).

Para IDS basados en red, ofrece al usuario la opción de Snort o Suricata (más información sobre ellos más adelante); para IDS basados en host (también conocidos como HIDS), ofrece Wazuh.

9. MOZDEF

La compañía famosa por Firefox construyó esta herramienta de automatización de incidentes de seguridad y respuesta a partir de otras herramientas de código abierto. Se lanzó por primera vez en 2014.

Cada servicio de su arquitectura se ejecuta en un contenedor Docker. Mozilla lo describe como un complemento SIEM que se ejecuta sobre Elasticsearch para el registro y Python para escribir nuevas reglas.

Según la documentación de MozDef, puede integrarse con una serie de proveedores de registros y exportar JSON a HTTP(S) o rabbit-mq. También puede vincularse con GuardDuty y AWS CloudTrail. Además de los mencionados anteriormente, enumeran las siguientes herramientas de código abierto como su base: Nginx, Meteor, MongoDB, VERIS (de Verizon), y varias herramientas relevantes para Python o JavaScript.

10. SNORT

Snort es un sistema de detección de intrusiones en red (NIDS) diseñado para Windows y Linux. Esto lo distingue de otros sistemas basados en host como OSSEC. Teniendo esto en cuenta, Snort no es necesariamente una alternativa a OSSEC u otros SIEM, sino un posible complemento.

Snort recibe su nombre por ser un rastreador de paquetes que "olfatea" las amenazas a la seguridad de las redes. Detecta e informa de los métodos de ataque, enviando así una alerta a syslog o a través de otro canal. Realiza análisis de tráfico en tiempo real junto con registros. Está diseñado para detectar una larga lista de diferentes vectores de ataque que incluye huellas dactilares de SO, DDOS, CGI, sondas SMB, desbordamientos de búfer y escaneos de puertos sigilosos. Utiliza OpenAppID para detectar aplicaciones.

Su creador, Martin Roesch, montó Sourcefire para gestionar el software para sus cientos de miles de usuarios. Sourcefire fue adquirida por Cisco en 2013, pero Snort conserva sus orígenes de código abierto (mientras que Cisco ha pasado a desarrollar alternativas comerciales basadas en el software original).

Su versión más reciente, 2.9.15.0, llegó en octubre de 2019. Algunas de sus deficiencias podrían ser abordadas por Snort 3.0 (actualmente en beta), incluida su falta de multihilo.

Snort es a menudo comparado con Suricata y podría servir como alternativa a él.

11. SURICATA

Alternativa común a Snort, ha recortado la base de usuarios del primero como sistema común de detección de intrusiones (IDS), procesamiento de PCAP, prevención de intrusiones y monitorización de redes. Es propiedad de la Open Information Security Foundation (OISF). En concreto, está construido a partir del lenguaje de scripting Lia, cuyos desarrolladores comercializan como un lenguaje pequeño, rápido e integrable.

Mantiene integraciones en YAML y JSON para otras bases de datos como Elasticsearch y Splunk.

Utiliza muchas de las mismas reglas que Snort, pero con algunas diferencias. En lugar de OpenAppID, puede utilizar la detección de la capa de aplicación para identificar el tráfico HTTP y SSH.

Como herramienta más reciente, también es más adepta a los problemas informáticos modernos. Soporta multihilo de forma nativa en lugar de la ejecución de Snort de múltiples instancias de un solo hilo.

No hay "un anillo que los gobierne a todos"

Una solución SIEM completa incluye la capacidad de recopilar información de varias fuentes de datos, retener esa información durante un largo periodo de tiempo, correlacionar entre diferentes eventos, crear reglas de correlación o alertas, analizar los datos y monitorizarlos con visualizaciones y cuadros de mando.

Al responder a muchos de estos requisitos, no es casualidad que la pila ELK sea utilizada por muchos de los sistemas SIEM de código abierto enumerados en este artículo. OSSEC Wazuh, SIEMonster, Metron -

todos tienen ELK bajo el capó. Pero por sí solo, ELK carece de algunos componentes SIEM clave, como las reglas de correlación y la gestión de incidentes.

Esa es parte de la razón que nos llevó a construir Logz.io Cloud SIEM, para crear un único panel a través del cual observar los eventos relevantes para la seguridad en sus registros. Basado principalmente en la pila ELK, se basa en la sabiduría que se ve en muchas soluciones. Combina datos de protecciones de puntos finales como Sophos y ESET, cortafuegos como SonicWall y Stormshield, MSSP y otros.

Basándonos en el análisis anterior, la simple conclusión es que no hay claros ganadores al título de "solución SIEM de código abierto todo en uno". Al implantar un sistema SIEM basado en las soluciones anteriores, lo más probable es que se encuentre limitado en cuanto a funcionalidad o que se combine con herramientas de código abierto adicionales.

Las herramientas de código abierto utilizadas para SIEM son versátiles y potentes. Pero requieren mucha experiencia y, sobre todo, tiempo para desplegarse correctamente. Por esta razón, las ofertas comerciales siguen dominando el panorama SIEM, incluso cuando las herramientas de código abierto son el núcleo de esas ofertas comerciales.

Tener el 80% de la solución SIEM en sus manos es mejor que tener que hacerlo todo uno mismo. Las soluciones comerciales se encargan de la instalación, la configuración básica y proporcionan filtros, configuraciones de correlación y diseños de visualización para los casos de uso más comunes. No subestime el valor de estas funciones comerciales: hay un número aparentemente ilimitado de cosas que supervisar en los centros de datos de hoy en día, y ninguno de nosotros tiene tiempo de configurar manualmente las aplicaciones para vigilarlas todas.