McAfee
Together is power.

Administración de eventos e información de seguridad (SIEM): cinco requisitos para resolver los grandes problemas de las empresas

Tras más de una década de uso en entornos de producción, las soluciones de administración de eventos e información de seguridad (SIEM) ya se consideran maduras. Funciones como la recopilación y correlación de eventos, las alertas y la demostración del cumplimiento de las normativas oficiales son básicas, y la mayoría de las soluciones SIEM las incorporan. Pero la situación está cambiando. Las empresas se enfrentan a nuevas amenazas, como los ataques selectivos y persistentes; nuevas tendencias, como el uso de móviles, la nube y la virtualización; y un cambio en las prioridades empresariales relacionado con la adquisición de clientes, la eficacia operativa y el ahorro de costes. Como resultado, las soluciones SIEM deben ofrecer funciones más avanzadas para resolver los grandes problemas de las empresas.

McAfee ha hablado con los usuarios de soluciones SIEM y les ha pedido que nos cuenten cuáles son sus principales problemas en relación a estas soluciones. Son cinco:

- Seguridad basada en Big Data
- Conocimiento de la situación
- Contexto en tiempo real
- Facilidad de uso
- Seguridad integrada

Para que las soluciones SIEM puedan conducir a estrategias de seguridad y gestión de riesgos más eficaces —especialmente porque se refieren a la mitigación de riesgos, adopción de tendencias y adecuación a las prioridades empresariales— es preciso abordar estos cinco problemas. A continuación se describe cada una de ellos, junto a los correspondientes análisis de casos de clientes y casos prácticos.

1. Seguridad basada en Big Data

La seguridad basada en los grandes volúmenes de datos, lo que se conoce como Big Data, es extremadamente valiosa, siempre que pueda utilizarse. Las soluciones SIEM anteriores no estaban diseñadas para integrar un número tan elevado de endpoints, redes y fuentes de datos, ni para procesar tasas de eventos tan altas ni mantener directivas de retención durante tanto tiempo. Por este motivo, las bases de datos relacionales y otras carencias de las soluciones SIEM heredadas, diseñadas principalmente para los eventos centrados en la red, no satisfacen las necesidades de seguridad de las infraestructuras de TI dinámicas actuales. No ofrecen la velocidad, capacidad de ampliación y escalabilidad necesarias para ser eficaces y útiles.

Caso práctico: sector público

Un gran organismo oficial pretendía aplicar análisis avanzados a grandes volúmenes de datos de seguridad almacenados en su enorme base de datos relacional de SIEM. Sin embargo, incluso la generación de los informes más sencillos llevaba horas, en algunos casos días, con lo que la solución SIEM del organismo resultaba impracticable para los análisis forenses.

Cuando cambiaron a McAfee® Enterprise Security Manager como solución SIEM, pudieron ampliar el número y los tipos de dispositivos integrados, agregando más datos y contextos centrados en los usuarios a sus análisis. Asimismo aumentó la tasa de eventos y los datos almacenados. Ahora, los informes se generan en cuestión de minutos, lo que mejora el proceso completo de análisis forense.

2. Conocimiento de la situación

Hace mucho tiempo las soluciones SIEM eran simplemente una herramienta para correlacionar eventos de distintos firewalls y sistemas de detección de intrusiones, y posteriormente posiblemente aplicar datos de evaluación de vulnerabilidades. Incluso hoy día, algunas SIEM se basan principalmente en los datos de flujo de red. Aunque todas estas fuentes son importantes, deben enriquecerse con datos contextuales y de aplicaciones, así como información de identidad. En caso contrario, se necesitarán más tiempo y recursos para poder entender y priorizar los eventos

Caso práctico: seguridad basada en Big Data

- Amplíe la obtención de datos con más vías de información de distintas fuentes.
- Realice análisis y análisis forenses sobre grandes conjuntos de datos.
- Realice optimizaciones para satisfacer los requisitos de velocidad y volumen de la seguridad basada en Big Data.
- Aumente la eficacia del personal y los procesos.

Caso práctico: conocimiento de la situación

- Mejore el conocimiento de la situación con más soluciones de identidad.
- Averigüe quién, cuándo, cómo, dónde y qué.
- Identifique cuánto tiempo, quién más y qué mas.
- Incluya activos BYOD, como portátiles y smartphones.

con los suficientes datos sobre la situación para poder realizar las acciones oportunas en el momento preciso.

Caso práctico: proveedor de servicios sanitarios

Un proveedor de servicios sanitarios regional adoptó el enfoque BYOD, o uso en el trabajo de dispositivos personales de los empleados, para que gracias al uso de tablets personales se pudiera incrementar la agilidad del personal. Sin embargo, a causa de incidentes ocurridos en el pasado, al proveedor le preocupaba la filtración de información privilegiada por parte de empleados. La solución anterior SIEM del proveedor no permitía averiguar qué usuarios interactuaban con los datos confidenciales independientemente del dispositivo; portátil, ordenador de sobremesa, tablet o equipo virtual.

Con McAfee Enterprise Security Manager, el proveedor se conectó a productos de administración de identidades y movilidad, Active Directory y LDAP, con el fin de obtener información sobre los usuarios y los dispositivos. La integración con almacenes de datos no estructurados, como bases de datos nativas, así como con sistemas de prevención de pérdida de datos (DLP) y de supervisión de la actividad de las bases de datos (DAM), le ofreció un conocimiento de la situación más global y permitió mitigar el riesgo de amenazas internas.

3. Contexto en tiempo real

Una de las primeras funciones de SIEM era la administración del registro: recopilación, almacenamiento y consulta de datos, con algunas otras funciones adicionales. Los registros siguen siendo esenciales en las soluciones SIEM, pero en la actualidad esta tecnología necesita también contexto en tiempo real.

Dos ejemplos de este tipo de contexto son McAfee Global Threat Intelligence (McAfee GTI) y McAfee Vulnerability Manager. McAfee GTI proporciona un servicio de reputación en tiempo real, basado en la nube, y McAfee Vulnerability Manager obtiene información de la empresa acerca de las vulnerabilidades de los activos.

Caso práctico: minorista

Una empresa minorista que figura en el índice Fortune 100, que no empleaba ninguna solución SIEM de producción ni ninguna solución de McAfee, llevó a cabo una prueba de concepto. En la primera semana, descubrió que más del 30 % del tráfico que intentaba acceder a su red procedía de fuentes malintencionadas y/o contenía cargas útiles maliciosas.

Gracias al uso de McAfee Enterprise Security Manager para correlacionar información de los eventos con McAfee GTI, el minorista identificó rápidamente los activos atacados en todas sus tiendas y centros de datos, y averiguó el tipo de ataques que recibía la organización. La solución McAfee SIEM determinó el máximo nivel de gravedad y, a continuación, priorizó una respuesta. La combinación de la solución SIEM con contexto en tiempo real permitió detectar la amenaza más rápidamente, establecer prioridades y aplicar soluciones.

4. Facilidad de uso

Las soluciones SIEM antiguas tienen arquitecturas muy rígidas y carecen de algunas funciones que son esenciales. Por ejemplo, no se pueden integrar fácilmente con dispositivos que no se admitían antes para poder utilizar la información. Las soluciones

Caso práctico: contexto en tiempo real

- Detecte las amenazas de dentro y fuera de su entorno.
- Mejore la información de SIEM con contexto en tiempo real.
- Reduzca la identificación de incidentes y los tiempos de respuesta.
- Identifique y priorice las amenazas con nuevas informaciones de seguridad.

Caso práctico: facilidad de uso

- Despliegue SIEM con listas blancas dinámicas y seguridad asistida por hardware para proteger los dispositivos de función fija.
- Simplifique los análisis forenses con análisis detallados personalizables.
- Integre SIEM con firewalls y sistemas de prevención de intrusiones (IPS) para obtener una respuesta a incidentes rápidamente.
- Alargue la vida de los activos heredados gracias a la mejora de la seguridad.

SIEM de próxima generación, sin embargo, se pueden personalizar fácilmente y, gracias a su flexibilidad, encajan en cualquier entorno. Por este motivo tienen tanto valor estratégico para muchas empresas.

Caso práctico: empresa de servicios públicos

Una empresa de servicios públicos necesitaba emplear controles de seguridad para impedir que ataques de tipo Stuxnet contra su infraestructura pudieran dejar sin suministro a millones de clientes. Con McAfee Enterprise Security Manager, la empresa consiguió tener un conocimiento de la situación en las áreas de TI empresariales, SCADA y sistemas de control industrial (ICS) con soporte nativo de dispositivos, aplicaciones y protocolos.

McAfee SIEM proporcionó al cliente las herramientas para realizar su propia integración personalizada con los dispositivos SCADA e ICS. Esto permitió la correlación de eventos, la detección de anomalías y el análisis de tendencias en las tres áreas. Además de la recopilación de eventos personalizada, el cliente pudo diseñar de manera rápida y fácil paneles, informes, reglas de correlación y alertas exclusivos. Así, la solución SIEM se convirtió en una herramienta de enorme valor para la seguridad, capaz de demostrar el cumplimiento de las normativas, garantizar la disponibilidad de los activos y, en definitiva, asegurar la continuidad del servicio.

5. Seguridad integrada

Si bien SIEM es un componente importante de cualquier iniciativa estratégica, es solamente uno de tantos. La integración de las distintas soluciones de seguridad y cumplimiento de normativas es más eficaz que el funcionamiento aislado de cada solución, además de que la falta de integración genera complejidades. Esta complejidad es la causa por la que la seguridad a menudo es una cuestión táctica, en lugar de estratégica y alineada con las prioridades de la empresa.

Caso práctico: servicios financieros

Una institución bancaria multinacional poseía gran cantidad de productos distintos de diferentes proveedores. Algunos de ellos eran productivos, pero otros no se usaban ni se mantenían con regularidad debido a escasez de recursos. El banco llegó a la conclusión de que mediante el empleo de tecnología SIEM junto con controles de endpoints, redes y datos, podía mitigar los riesgos de forma más eficaz y reducir los costes, al tiempo que conseguiría que la seguridad estuviera más adaptada a la actividad empresarial.

El banco redujo el número de proveedores y logró economías de escala. Pudo disminuir los costes de formación y el número de agentes, consolas y servidores, entre otros. De esta forma, bajaron también los costes de contratos y numerosos gastos asociados. Más allá del ahorro de costes, el banco garantizó la integración total de las soluciones existentes y futuras con McAfee Enterprise Security Manager, con el fin de mejorar los controles y la visibilidad del estado de su seguridad.

Caso práctico: seguridad integrada

- Simplifique el flujo de operaciones y la seguridad.
- Elimine las complejidades con la automatización y personalización sencilla.
- Mejore la visibilidad y el conocimiento de la situación con soluciones de seguridad que funcionan juntas.
- Proporcione mejor seguridad con información e integración.

Consideraciones clave

- ¿Qué importancia tiene la capacidad para gestionar la recopilación, almacenamiento, acceso, procesamiento y análisis de datos seguridad basada en Big Data?
- ¿Están los implicados en la seguridad obteniendo la información que necesitan cuando la necesitan para tomar decisiones fundamentadas y las acciones oportunas?
- ¿Cuenta su equipo de seguridad con contexto en tiempo real para identificar los riesgos y los ataques antes de que causen daños?
- ¿Cuál sería el impacto para la seguridad y los recursos si usara una solución SIEM con análisis de datos intuitivos y vistas que se pudieran personalizar fácilmente?
- ¿Cómo mejoraría la integración en su infraestructura la seguridad, la visibilidad, los procesos y la capacidad de respuesta?

Lo que hace una década funcionaba con las soluciones SIEM, hoy día simplemente no satisface las necesidades actuales. Con los nuevos requisitos relativos a los grandes volúmenes de datos, información de seguridad, conocimiento de la situación, rendimiento, facilidad de uso e integración, los casos prácticos de SIEM se han multiplicado. Las soluciones SIEM deben reducir la complejidad; no crearla. Pídale más a su solución SIEM.

En la actualidad, las soluciones SIEM funcionan como parte de una infraestructura de seguridad conectada, más grande, en la que se alinean las prioridades de seguridad y las del negocio. Resultan fundamentales para que la seguridad sea más estratégica y para obtener un valor empresarial real.

Para obtener más información acerca de las soluciones SIEM de McAfee, visite: **www.mcafee.com/es/products/siem/index.aspx**.

Seguridad integrada

McAfee ofrece una infraestructura unificada e integrada para cientos de productos, servicios y partners que permite compartir conocimientos y datos sobre el contexto en tiempo real, y actuar conjuntamente con el fin de garantizar la seguridad de la información y las redes. Cualquier organización debe mejorar su estado de la seguridad y minimizar los costes operativos a través de los conceptos innovadores de la plataforma, procesos optimizados y ahorros concretos.

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es