Informe oficial

Sentinel

La guía completa sobre gestión de eventos y registros

escrita por el Dr. Anton Chuvakin, con el patrocinio de NetIQ

Todo el mundo tiene registros, lo que significa que todo el mundo tiene que ocuparse de ellos, aunque solo sea porque así lo exigen las obligaciones normativas. En esta guía, el Dr. Anton Chuvakin analizará la relación existente entre SIEM y la gestión de registros, concentrándose no solo en las diferencias técnicas y los distintos usos, sino también en el diseño de sus implantaciones conjuntas. Ofrecerá, asimismo, recomendaciones para las empresas que han implantado una solución de gestión de registros o de SIEM, con el objeto de que puedan planificar su estrategia y plan de evolución para mejorar, optimizar y ampliar su implantación. Aconsejará también una estrategia y plan de evolución para las empresas que ya hayan implantado ambas tecnologías.

NetIQ

Índice

página

Introducción

La tecnología de gestión de la información y los eventos de seguridad, o SIEM, existe desde finales de los 90, pero siempre ha sido polémica de algún modo en el sector de la seguridad debido a su promesa inicial de una vista unificada de la seguridad, lo que se sumó a la lentitud de la adopción en las empresas de menor tamaño. Más recientemente, la tecnología de SIEM tradicional se ha unido al uso extendido de la de gestión de registros, que se centra en la recopilación de una variedad más amplia de registros con fines múltiples; desde la respuesta a incidencias de seguridad hasta la conformidad normativa, pasando por la gestión del sistema o la resolución de problemas de aplicaciones.

En este informe analizaremos la relación existente entre la tecnología de SIEM (gestión de la información y los eventos de seguridad) y la de gestión de registros, concentrándonos no solo en las diferencias técnicas y los distintos usos, sino también en el diseño de sus implantaciones conjuntas. Por ejemplo, ¿cuál de ellas debería implantar si necesita cumplir los requisitos de registro de la norma de seguridad de datos del sector de pagos con tarjeta (PCI-DSS)? ¿Cuál de estas tecnologías es más adecuada para optimizar la respuesta a incidencias y los procedimientos de investigación? ¿Cuál de ellas le proporcionará información en tiempo real sobre los ataques? Ofreceremos, asimismo, recomendaciones para las empresas que han implantado una solución de gestión de registros o de SIEM, con el objeto de que puedan planificar su estrategia y plan de evolución para mejorar, optimizar y ampliar su implantación. Aconsejaremos también una estrategia y un plan de evolución para las empresas que ya hayan implantado ambas tecnologías.

Las herramientas de SIEM aparecieron por primera vez en el mercado en 1997. Originalmente se utilizaron para reducir el número de falsos positivos de los sistemas de detección de intrusiones en la red (NIDS), muy frecuentes en los sistemas NIDS por aquel entonces. La instalación de estas herramientas era compleja, y también lo era su uso, por lo que solo las empresas de mayor tamaño las utilizaban con los programas de seguridad más avanzados. A finales de los noventa, el mercado

se calculaba en unos cuantos millones de dólares; en la actualidad, algunos analistas informan de que va camino de alcanzar cifras de miles de millones de dólares en los próximos años. Las herramientas de SIEM actuales, como NetIQ Sentinel, son utilizadas por empresas de todos los tamaños, desde compañías que figuran en la lista Fortune 1000 o Global 2000, hasta empresas de tamaño pequeño y mediano (Pymes).

Antes de empezar nuestro análisis, debemos definir *SIEM* y *gestión de registros,* y explicar en qué se diferencian. *SIEM* abarca la recopilación de registros relevantes, así como su adición, normalización y retención; la recopilación de datos de contexto; el análisis, con correlación y establecimiento de prioridades incluidos; la presentación, con informes y visualización incluidos; y el flujo de trabajo relacionado con la seguridad y el contenido de seguridad asociado. Todos los casos de uso de SIEM se centran en la seguridad de la información, la seguridad de la red, la seguridad de los datos y la conformidad normativa.

Por otro lado, la *gestión de registros* incluye la recopilación exhaustiva de registros, así como su adición, la retención de registros originales (en bruto, sin modificar), el análisis de textos de registros, la presentación (normalmente en forma de búsqueda pero también de informes), el flujo de trabajo relacionado y el contenido. Con la gestión de registros, los casos de uso son amplios y cubren todos los posibles usos de los datos de registro mediante TI y mucho más.

La diferencia fundamental que se sigue de las definiciones anteriores radica en el hecho de que SIEM se concentra en la seguridad —la primera de las palabras que componen su nombre en inglés (Security Information and Event Management)— y el uso de información de TI diversa con fines de seguridad. La gestión de registros, en cambio, se centra en los registros y la amplia gama de usos para los datos de registro, tanto dentro como fuera de la esfera de la seguridad.

SIEM:

- Recopilación, adición, normalización y retención de registros relevantes
- Recopilación de datos contextuales
- Análisis (incluidos el establecimiento de prioridades y la correlación)
- Presentación (Incluidas la generación de informes y la visualización)
- Flujo de trabajo relacionado con la seguridad y contenido de seguridad asociado
- Seguridad de información, seguridad de red, seguridad de datos y conformidad con la normativa

Funciones definitorias de la gestión de la información y los eventos de seguridad

Vamos a comentar más detenidamente las características que definen la tecnología de SIEM; la mayoría de los usuarios buscarán estas funciones al elegir un producto de SIEM. Las funciones son:

- **Recopilación de datos de contexto y registros.** *Esta función incluye la recopilación de registros y datos de contexto, como la información de identidad o los resultados de la evaluación de la vulnerabilidad, utilizando una combinación de métodos sin agente y basados en agente.*
- **Normalización y clasificación.** *Esta función abarca la conversión de los registros originales recopilados a un formato universal para su uso dentro del producto de SIEM. Los eventos también se clasifican en bandejas útiles, como "Cambio de configuración", "Acceso a archivos" o "Ataque de desbordamiento de buffer".*
- **Correlación.** *Esta función incluye la correlación basada en reglas, correlación estadística o algorítmica, así como otros métodos que incorporan la relación de distintos eventos entre sí, y entre eventos y datos de contexto. La correlación puede ser en tiempo real, aunque no todas las*

Gestión de registros:

- Recopilación exhaustiva, adición y retención de registros originales (en bruto, sin modificar)
- Análisis de textos de registros
- Presentación, normalmente en forma de búsqueda pero también de informes
- Contenido y flujo de trabajo relacionado
- Casos de uso amplios que cubren todos los posibles usos de los datos de registro mediante TI y mucho más

herramientas son compatibles con la correlación en tiempo real y, en su lugar, se centran en la correlación de datos históricos de sus bases de datos. Hay otros métodos de análisis de registro que a veces se agrupan también bajo la etiqueta de correlación.

- **Notificaciones y alertas.** *Esta función incluye la activación de notificaciones o alertas para los operadores o gerentes. Entre los mecanismos de alerta habituales están el correo electrónico, el servicio de mensajes cortos (SMS) e incluso los mensajes de Protocolo Simple de Administración de Red (SNMP).*
- **Establecimiento de prioridades.** *Incluye distintas funciones que ayudan a destacar los eventos importantes de los eventos de seguridad con menor importancia. Esto se puede lograr mediante la correlación de eventos de seguridad y datos de vulnerabilidad, u otra información sobre activos. Los algoritmos de establecimiento de prioridades a menudo usan también la información sobre importancia facilitada por la fuente de registros original.*
- **Vistas en tiempo real.** *Esta función cubre las consolas y pantallas de supervisión de la seguridad que utiliza el personal de operaciones. Estas pantallas muestran a los analistas la información recopilada, así como los resultados de correlación, en tiempo casi real. Los datos históricos y archivados también se pueden suministrar a estas vistas.*
- **Informes.** *Los informes e informes programados abarcan todas las vistas históricas de los datos que el producto de SIEM recopila. Algunos productos también cuentan con un mecanismo para la distribución de informes al personal de seguridad o gestión de TI, ya sea a través de correo electrónico o mediante un portal Web seguro dedicado a tal propósito.*
- **Flujo de trabajo de función de seguridad.** *Esto cubre las funciones de gestión de incidencias, como la apertura de casos y la ejecución de tareas de investigación, así como la ejecución automática o semiautomática de tareas típicas en operaciones de seguridad. Algunos productos también incluyen funciones de colaboración que permiten a varios analistas trabajar en la misma respuesta de seguridad.*

La función anterior puede encontrarse en la mayoría de los productos comerciales de SIEM que están disponibles en el mercado actualmente. No obstante, la mayoría de los productos tienen puntos débiles y puntos fuertes, además de funciones adicionales que aportan ese ingrediente secreto.

Funciones definitorias de la gestión de registros

Comencemos por considerar las funciones definitorias de un sistema de gestión de registros. Estas incluyen:

- **Recopilación de datos de registros.** *Esta función abarca la recopilación de todos los registros mediante métodos basados en agente, sin agente, o una combinación de ambos.*
- **Retención eficaz.** *Aunque recopilar y guardar datos de registro no parezca un enorme desafío de ingeniería, recopilar gigabytes, e incluso terabytes, de datos de registro de forma eficaz, y retenerlos a la vez que se proporciona una búsqueda y un acceso rápidos a ellos, no es una tarea insignificante. Dado que muchas normativas incluyen disposiciones específicas sobre la retención de los datos de registros, a menudo para periodos de varios años, se trata de una función esencial en un sistema de gestión de registros.*
- **Búsqueda.** *Constituye el principal modo de acceder a la información en todos los registros, incluidos los procedentes de aplicaciones personalizadas. La búsqueda es imprescindible para el uso de los registros en investigación, el análisis forense de los registros y la localización de fallos, al tiempo que los registros se utilizan para la resolución de problemas de aplicaciones. Una interfaz de búsqueda interactiva limpia y fiable es, por tanto, esencial en un sistema de gestión de registros.*

- **Análisis o indexación de registros.** *Estos son los componentes clave de un sistema de gestión de registros. La indexación puede multiplicar la velocidad de las búsquedas por cien, literalmente. La tecnología de indexación crea una estructura de datos denominada índice que permite realizar búsquedas por palabra clave y booleanas muy rápidas en todo el almacén de registros. A veces, la indexación se utiliza para facilitar otras técnicas de análisis de texto completo. Considérela como el equivalente de Google para los registros. No toda las herramientas de gestión de registros son compatibles con la indexación o anuncian índices de recopilación de registros que no dan cuenta de la indexación, así que es importante tener cuidado con las afirmaciones de los proveedores.*
- **Informes e informes programados.** *Estas funciones abarcan todos los datos recopilados por el producto de gestión de registros y son similares a los informes de SIEM. La eficacia de la información, ya sea con fines de seguridad, de conformidad u operativos, puede ser el alma de una solución de gestión de registros, o su talón de Aquiles. Los informes deben ser rápidos, personalizables y fáciles de usar con una amplia gama de propósitos. La diferencia entre búsquedas e informes es bastante clara: la búsqueda se produce sobre todos los registros disponibles, recopilados en bruto, en su formato original (como Google trata las páginas Web), mientras que el informe opera sobre registros organizados en una base de datos (como una hoja de cálculo de Excel). Es necesario evaluar detenidamente la facilidad con la que se puede crear un informe personalizado en una herramienta de gestión de registros. Es aquí donde muchas soluciones no dan la talla, ya que requieren que sus operadores estudien los aspectos esotéricos de sus estructuras de datos de almacenamiento de registros antes de poder personalizar los informes.*

No toda las herramientas de gestión de registros son compatibles con la indexación o anuncian índices de recopilación de registros que no dan cuenta de la indexación, así que es importante tener cuidado con las afirmaciones de los proveedores.

Comparemos, ahora, las características y funciones de SIEM y de la gestión de registros a un nivel superior.

Comparación de nivel superior: SIEM frente a la gestión de registros

En la tabla que aparece a continuación, mostramos las áreas clave de funciones y explicamos las diferencias entre SIEM y la gestión de registros:

Funcionalidad	Gestión de la información y los eventos de seguridad (SIEM)	Gestión de registros
Recopilación de registros	Recopilación de registros de seguridad	Recopilación de todos los registros, incluidos los operativos y de aplicaciones personalizadas
Retención de registros	Retención limitada de datos de registro normalizados y analizados	Retención de datos de registro en bruto y analizados durante períodos prolongados
Informes	Generación de informes centrados en la seguridad, generación de informes en tiempo real	Generación de informes de uso extenso e informes históricos
Análisis	Correlación, evaluación de amenazas, establecimiento de prioridades de eventos	Análisis de texto completo, etiquetado
Alertas y notificaciones	Informes avanzados centrados en la seguridad	Alerta sencilla sobre todos los registros
Otras funciones	Gestión de incidentes, otros análisis de datos de seguridad	Alta capacidad de ampliación para la recopilación y búsqueda

Repasemos ahora cómo se utilizan las tecnologías de SIEM y las de gestión de registros.

Tres tipos principales de casos de uso:

- Seguridad, detección e investigación
- Conformidad con las normativas (globales) y políticas (locales)
- Resolución de problemas operativos, de sistema y red, y operaciones normales

Recientemente, la tecnología de SIEM tradicional se ha unido al uso extendido de la de gestión de registros, que se centra en la recopilación de una variedad más amplia de registros con fines múltiples; desde la respuesta a incidencias de seguridad hasta la conformidad normativa, pasando por la gestión del sistema o la resolución de problemas de aplicaciones.

Casos de uso de las tecnologías de SIEM y de gestión de registros

Antes de comentar la arquitectura conjunta de la gestión de la información y los eventos de seguridad y la gestión de registros, debemos presentar brevemente casos de uso típicos que requieren la implantación de un producto de SIEM en la empresa de un cliente. Comenzaremos en el nivel más alto de los tres principales tipos de casos de uso:

1. **Seguridad, detección e investigación.** A veces denominada gestión de amenazas, se centra en la detección de ataques, infecciones de malware, sustracción de datos y otros problemas de seguridad, así como en ofrecerles respuesta.
2. **Conformidad con las normativas (globales) y políticas (locales).** Se centra en satisfacer los requisitos de diversas leyes, mandatos y marcos, además de las políticas corporativas locales.
3. **Resolución de problemas operativos, de sistema y red, y operaciones normales.** Este caso de uso es específico para la mayoría de las soluciones de gestión de registros y está relacionado con la investigación de problemas del sistema, además de la supervisión de la disponibilidad de los sistemas y aplicaciones.

En un nivel más detallado, los casos de uso de seguridad y conformidad se clasifican en varios escenarios posibles. Revisémoslos más detenidamente.

El primer escenario posible es el del centro de operaciones de seguridad tradicional (por sus siglas en inglés, SOC). Este suele hacer un uso intensivo de las funciones de SIEM, como las vistas y la correlación en tiempo real. Una organización cliente de SIEM tendrá analistas en línea con horario ininterrumpido que se encargarán de realizar el seguimiento de las alertas de seguridad en el momento en que se producen. Este fue el caso de uso original de la tecnología de SIEM, cuando daba sus primeros pasos en la década de los noventa. Hoy día, ha quedado relegado exclusivamente a las empresas de mayor tamaño.

El siguiente caso de uso recibe a veces el nombre de “mini SOC”. En este, el personal de seguridad utiliza vistas retrasadas, no en tiempo real, para comprobar los problemas de seguridad (los analistas “llegan por la mañana”). Puede que los analistas se encuentren en línea algunas horas durante el día y solo revisen las alertas e informes conforme se requiera, y no en tiempo casi real, a menos que los eventos sucedan mientras han iniciado sesión en el producto.

El tercer escenario es el de un SOC automatizado en el que una empresa configura su solución de SIEM para que active alertas basadas en reglas y, acto seguido, se olvida del tema hasta que se produce una alerta. Los analistas nunca inician sesión, a menos que haya necesidad de investigar una alerta, revisar informes con frecuencia semanal o mensual, o llevar a cabo otro tipo de tareas excepcionales. Este es el caso de uso que muchas empresas de pequeño tamaño desean y que pocos productos de SIEM pueden proporcionar, al menos no sin una personalización extensa. Vale la pena añadir que muchos productos de SIEM se venden con la expectativa de que sean un SOC automatizado, pero tales expectativas raramente llegan a cumplirse.

La resolución de problemas de las aplicaciones y la administración de sistemas constituyen dos casos de uso adicionales importantes de los sistemas de gestión de registros.

Las tecnologías de gestión de registros desempeñan también una función en otros escenarios fuera del contexto de la seguridad. La resolución de problemas de las aplicaciones y la administración de sistemas constituyen dos casos de uso adicionales importantes de los sistema de gestión de registros. Cuando la aplicación se ha implantado y se han configurado sus registros, el sistema de gestión de registros se utiliza para revisar rápidamente errores y registros de excepciones. También revisará los resúmenes de la actividad normal de la aplicación para determinar el estado de salud de la aplicación y resolver las posibles irregularidades.

Un escenario incluido en esta última categoría es el de la información del estado de conformidad. En este caso, los analistas o gestores de la seguridad revisan los informes centrándose en los problemas de conformidad. La revisión se produce con carácter semanal o mensual, o según lo requerido por una norma específica. Esta no tiene por qué centrarse necesariamente en la seguridad o las operaciones. Este caso de uso suele constituir una fase de transición, y es muy probable que la empresa desarrolle con el tiempo uno de los casos de uso mencionados previamente. Las herramientas de gestión de registros se implantan con mayor frecuencia para este escenario, pero no es raro que también se utilice un producto de SIEM con fines de conformidad. Los requisitos de retención de registros a largo plazo a menudo representan un desafío para la implantación.

Dado que los registros son muy importantes para cumplir las obligaciones de conformidad, consideremos detenidamente unas cuantas normas.

PCI-DSS

La norma de seguridad de datos del sector de pagos con tarjeta (por sus siglas en inglés, PCI-DSS) se aplica a las empresas que gestionan transacciones de tarjetas de crédito. Obliga a registrar detalles específicos, retener los registros y llevar a cabo procedimientos de revisión de registros diarios.

Aunque el registro está presente en todos los requisitos del sector de pagos con tarjeta (PCI), el requisito número 10 de la norma PCI-DSS está dedicado a los registros y su gestión. De acuerdo con este requisito, los registros para todos los componentes del sistema deben revisarse con una frecuencia diaria, como mínimo. Asimismo, la norma PCI-DSS establece que la empresa debe garantizar la integridad de sus registros mediante la implantación de software de supervisión de la integridad de los archivos y detección de cambios en los registros. También estipula que los registros de los sistemas que abarca se guarden al menos durante un año.

La Ley de tecnología de la información de salud para la salud económica y clínica de 2009 (por sus siglas en inglés, HITECH) fomentará las implantaciones de la HIPAA en los años venideros.

FISMA

La ley federal de gestión de la seguridad de la información de 2002 (por sus siglas en inglés, FISMA) hace hincapié en la necesidad de que las agencias federales desarrollen, documenten e implanten un programa para toda la empresa con el fin de proteger los sistemas de información que respaldan sus operaciones y activos. La publicación especial del Instituto Nacional de Normas y Tecnología (por sus siglas en inglés, NIST) 800-53, Controles de seguridad recomendados para los sistemas de información federales, describe los controles de gestión de registros, incluyendo la generación, revisión, protección y retención de los informes de auditoría, junto con las medidas necesarias en el caso de que se produzca un fallo de auditoría.

La publicación especial 800-92 del NIST, Guía para la gestión de registros de seguridad informática, simplifica la conformidad con FISMA y garantiza que se dedica completamente a la gestión de registros. Describe la necesidad de una gestión de registros en las agencias federales, así como los modos de establecer y mantener infraestructuras de gestión de registros adecuadas y eficaces que incluyan generación, análisis, almacenamiento y supervisión de registros. Esta publicación del NIST comenta la importancia de analizar los distintos tipos de registros de fuentes diferentes y de definir con claridad las funciones y responsabilidades de los equipos e individuos que participan en la gestión de registros.

HIPAA

La Ley de transferibilidad y responsabilidad de seguros médicos de 1996 (por sus siglas en inglés, HIPAA) resume las normas de seguridad relevantes para la información sanitaria. La publicación especial 800-66 del NIST, Una guía de recursos introductoria para la implantación de la regla de seguridad de la HIPAA, detalla los requisitos de la gestión de registros para la seguridad de la información sanitaria protegida por medios electrónicos. La sección 4.1 de esta publicación describe la necesidad de regular la revisión de la actividad del sistema de información, como los registros de auditoría, los informes de acceso y los informes de seguimiento de incidencias de seguridad. La sección 4.22 especifica que debe retenerse la documentación de acciones y actividades durante al menos seis años. A veces, los registros se consideran parte de este tipo de documentación. La Ley de tecnología de la información de salud para la salud económica y clínica de 2009 (por sus siglas en inglés, HITECH) fomentará las implantaciones de la HIPAA en los años venideros.

Empresas de todos los tamaños usan las herramientas de SIEM actuales, como NetIQ® Sentinel™, desde compañías que figuran en la lista Fortune 1000 o Global 2000, hasta empresas de tamaño pequeño y mediano (Pymes).

Tendencias tecnológicas

La tecnología de SIEM tiene más de 10 años de antigüedad. Ha atravesado numerosas fases sobre las que podríamos escribir un informe técnico completo. En lugar de eso, vamos a destacar unas cuantas tendencias de esta tecnología. A pesar de que en sus orígenes la tecnología de SIEM se dirigió a grandes empresas de nivel mundial y a agencias gubernamentales confidenciales, continúa extendiéndose a los mercados de empresas más pequeñas. Numerosos analistas predijeron que los principales proveedores de soluciones de SIEM estarían compitiendo en los mercados de tamaño medio para 2011. Como resultado, se han obtenido mejores herramientas de gestión de la seguridad para los clientes de menor tamaño.

Otra tendencia es la aceptación de funciones separadas para la tecnología de SIEM y la de gestión de registros. La mayoría de los proveedores de soluciones de SIEM también ofrecen ahora soluciones de gestión de registros. Esto también respalda la ampliación de usos para las herramientas de SIEM a fin de abarcar, entre otros, las operaciones de TI, el análisis del fraude, la resolución de problemas de aplicaciones y los usos en GRC (Gobierno, Gestión de riesgos y conformidad) de TI para objetivos de gobierno de alto nivel y medición del riesgo.

También estamos siendo testigos del inicio de la convergencia entre las operaciones y la gestión de TI con la gestión de la seguridad. Aunque los analistas llevan varios años prediciendo esta tendencia, no se ha materializado por completo hasta ahora. A pesar de este dato, muchos prevén que la tendencia de convergencia entre la gestión de la seguridad y la gestión de las operaciones de TI va a continuar, y las herramientas de seguridad estarán más ligadas a las herramientas operativas de TI, como la gestión de redes y sistemas.

Muchos prevén que la tendencia de convergencia entre la gestión de la seguridad y la gestión de las operaciones de TI va a continuar, y las herramientas de seguridad estarán más ligadas a las herramientas operativas de TI, como la gestión de redes y sistemas.

Escenario posible de las tecnologías de SIEM y de gestión de registros

Este estudio de caso abarca la implantación de una solución de SIEM y de gestión de registros con el fin de satisfacer los requisitos de la norma PCI-DSS en una cadena comercial minorista de tamaño considerable. El comerciante decidió implantar una solución de gestión de registros comerciales cuando su asesor del sector de pagos con tarjeta sugirió que sería necesaria para superar una evaluación. Un proveedor de gestión de registros sugirió que el comerciante adquiriera una solución de gestión de registros, junto con una de SIEM. Así, pasó de no hacer nada con sus registros a ejecutar un sistema de gestión de registros avanzado con correlación en tiempo real.

Muchas empresas han implantado las dos o están considerando mejorar una implantación existente de una de estas tecnologías con la otra.

El proyecto llevó varios meses y siguió una estrategia por fases. Partiendo de una evaluación inicial del riesgo, el personal de TI del comerciante decidió llevar a cabo la implantación desde fuera hacia dentro. Comenzaron desde el cortafuegos de red perimetral (DMZ) y fueron avanzando mediante la introducción de registros adicionales en un sistema de gestión de registros, mientras que, de forma simultánea, se definían reglas de correlación y ejecutaban informes desde el paquete de conformidad con la norma PCI-DSS del proveedor. A medida que fueron aprendiendo a responder a las alertas, sus procesos maduraron y empezaron a utilizar más las funciones de SIEM.

En general, el proyecto representó una implantación eficaz de los requisitos de registro del sector de pagos con tarjeta. La empresa superó airosa la evaluación del PCI y recibió elogios por su enfoque completo orientado al registro y la supervisión de la seguridad. Asimismo, el equipo de seguridad consiguió defender que su implantación de SIEM para PCI resuelve de hecho mandatos de conformidad adicionales, ya que la norma PCI-DSS incluye un nivel de detalle superior que abarca, esencialmente, las mismas áreas que la gestión de TI. Al mismo tiempo que las herramientas de gestión de registros reforzaron las capacidades operativas y la eficacia general de TI, la tecnología de SIEM proporcionó a la empresa la base de su capacidad futura de detección y respuesta en tiempo real.

Diseño de la solución de gestión de registros y de SIEM

Dadas las diferencias entre ambas tecnologías, muchas empresas han implantado las dos, o están considerando mejorar una implantación existente de una de estas tecnologías con la otra. ¿Cuáles son algunas de las arquitecturas conjuntas comunes de las tecnologías de SIEM y de gestión de registros?

Nos referiremos al escenario más habitual como el de “escudo SIEM”. Muchas de las empresas que implantaron soluciones de SIEM legadas intentaron enviar demasiados datos a sus soluciones, lo que hizo que las sobrecargaran y, probablemente, perdieran datos y funciones fundamentales. Resolvieron este problema adquiriendo también una herramienta de gestión de registros e implantándola por delante de su solución de SIEM.

fig. 1

En este caso, una herramienta de gestión de registros, que de manera natural posee mayor capacidad de ampliación, se implanta por delante de una solución de SIEM a modo de escudo y filtro para proteger la herramienta de SIEM, que tiene menor capacidad de ampliación, de los flujos de registros extremos. No es poco corriente que solo se envíe el décimo evento recibido por el escudo de registros a una solución de SIEM que se oculta detrás. Al mismo tiempo, la herramienta de gestión de registros archiva todos los eventos recibidos. Por ejemplo, si el volumen de registros total equivale a 40 000 mensajes de registro por segundo, la herramienta de SIEM recibe solo 4000 mensajes por segundo.

No es poco corriente que solo se envíe a una solución de SIEM que se oculta detrás el décimo evento recibido por el escudo de registros. Al mismo tiempo, la herramienta de gestión de registros archiva todos los eventos recibidos.

fig. 2

Otro escenario posible surge cuando la gestión de registros se implanta primero para crear una plataforma de registros empresarial. Después, se añade la solución de SIEM como una de las aplicaciones de la plataforma. Este escenario se puede denominar “crecimiento hasta SIEM" y constituye hasta el 50 % de las implantaciones de SIEM actuales. Este es el caso cuando la empresa adquiere una herramienta de gestión de registros y, poco a poco, se da cuenta de que necesita correlación, visualización, supervisión y flujos de trabajo, entre otras opciones, y desarrolla la capacidad para utilizarlas. Tal escenario es el camino más lógico para la mayoría de las empresas, como comentamos más ampliamente en este informe.

Si una empresa se da cuenta de que necesita correlación, debe recopilar y guardar todos los registros, y contar con la opción de ejecutar búsquedas eficaces y análisis de datos en bruto.

Ser capaz de responder mejor debe ocurrir antes de que uno se vea forzado a ofrecer una respuesta más rápida. Es mucho más sencillo estar preparado para responder que para supervisar.

En el siguiente caso, las tecnologías de SIEM y de gestión de registros se implantaron juntas y a la vez. Se trata de un "escenario emergente", porque la mayoría de los clientes ahora adquieren las dos soluciones al mismo tiempo y, normalmente, del mismo proveedor. No cabe duda de que, si una empresa se da cuenta de que necesita correlación, debe recopilar y guardar todos los registros, y contar con la opción de ejecutar búsquedas eficaces y análisis de datos en bruto.

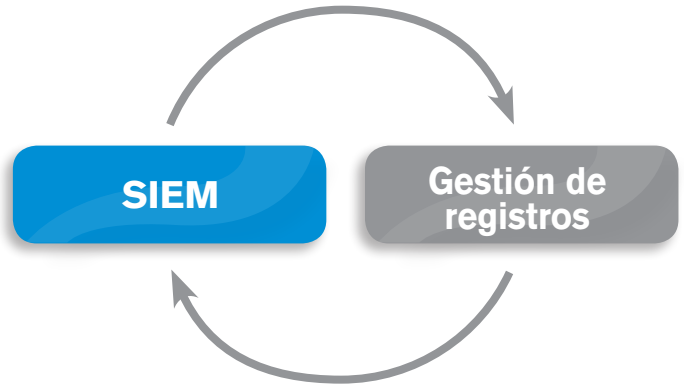

fig. 3

A continuación se presenta una implantación de SIEM con el producto de gestión de registros como archivo para registros procesados, entre otros. Este escenario se da cuando alguien adquiere una solución de SIEM de gran tamaño para la supervisión de la seguridad y con el tiempo se da cuenta de que falta algo. Como consecuencia, se implanta una herramienta de gestión de registros en la que volcar todos los registros y realizar el análisis de los registros en bruto que la solución de SIEM rechaza, como los registros que no sabe cómo organizar, normalizar o clasificar. Esto conduce a un caso de uso ampliado, desde la supervisión de la seguridad hasta la respuesta de incidencias y la conformidad con la norma PCI-DSS.

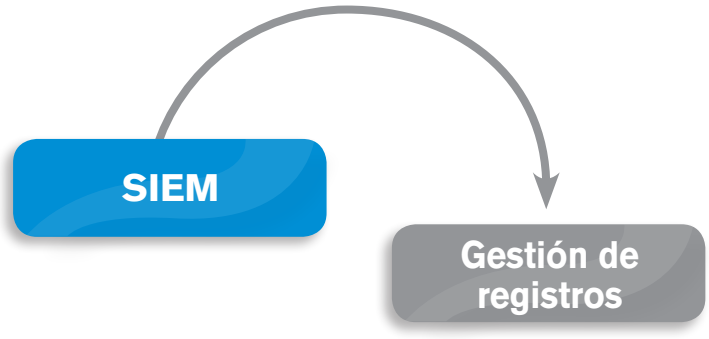

fig. 4

Además, existen numerosos escenarios de implantaciones solo de gestión de registros (todavía en aumento) y algunas de SIEM exclusivamente (que probablemente disminuyan).

¿Cómo empezar? ¿Con la solución de SIEM o con la de gestión de registros?

Afortunadamente, la pregunta de qué tecnología debe implantarse primero se responde fácilmente. Si tiene registros, necesita una solución de gestión de registros. Esto se aplica por igual tanto a las empresas con un solo servidor como a las que tienen 100 000. No cabe duda de que la tecnología que implanten para gestionar sus registros será diferente, pero la existencia de registros significa que necesitan una solución de gestión de registros. Por ejemplo, si tiene que revisar los registros de una sola máquina, normalmente serán suficientes las herramientas integradas del sistema operativo. Por otra parte, si su volumen de registros diario alcanza la impresionante cifra de 100 GB (lo que no es imposible), será necesario descubrir herramientas sofisticadas y, por tanto, caras.

En una publicación reciente de Gartner titulada “How to Implement SIEM Technology” (Cómo implantar tecnología de SIEM) (Gartner 2009), se recomienda sin reservas implantar funciones de gestión de registros antes de intentar una implantación de gestión de eventos en tiempo real a gran escala. Además, se aclara que, cuando la tecnología de SIEM está centrada en la conformidad, se recomienda el mismo orden de implantación: “las primeras fases de una implantación de SIEM que esté impulsada fundamentalmente por el PCI implantaría funciones de gestión de registros para los sistemas comprendidos en la evaluación del PCI”. El tema de fondo es que ser capaz de responder mejor tiene que preceder a la necesidad de responder con mayor rapidez.

Si tiene registros, necesita una solución de gestión de registros. Esto se aplica por igual tanto a las organizaciones con un solo servidor como a las que tienen 100 000.

En una publicación reciente de Gartner titulada “How to Implement SIEM Technology" (Cómo implantar tecnología de SIEM) (Gartner 2009), se recomienda sin reservas implantar funciones de gestión de registros antes de intentar una implantación de gestión de eventos en tiempo real a gran escala.

Antes de implantar una solución de SIEM, pregúntese en qué medida cuenta con una seguridad en tiempo real.

¿Qué ocurre con aquellas que ya han implantado herramientas de SIEM legadas? En este caso, lo más inteligente es considerar la tecnología de gestión de registros a la mayor brevedad. Ser capaz de revisar una colección completa de informes de registro mejorará sus capacidades de investigación y les ayudará a cumplir los mandatos de conformidad.

¿Todas las empresas tienen todas que progresar desde una solución de gestión de registros a otra de SIEM?

¿Qué ocurre después de que una organización implante una herramienta de gestión de registros y empiece a utilizarla eficazmente en seguridad y conformidad, así como con fines operativos? El progreso natural y lógico para las empresas es pasar de la gestión de eventos en tiempo casi real a la implantación de una herramienta de SIEM.

Este informe es el primer documento que formula el criterio de progresión para dicha implantación. Las empresas que realizan el tránsito demasiado pronto, desperdician tiempo y esfuerzos, y no consiguen mayor eficacia en sus operaciones de seguridad. Sin embargo, esperar demasiado tiempo también implica que las organizaciones nunca desarrollen las capacidades se seguridad que necesitan.

De manera resumida, los criterios son los siguientes:

- **Capacidad de respuesta.** *La empresa debe estar preparada para responder a las alertas poco después de que se produzcan.*
- **Capacidad de supervisión.** *La empresa debe tener, o empezar a desarrollar, una capacidad de seguimiento de la seguridad mediante la creación de un centro de operaciones de seguridad o, como mínimo, a través de un equipo dedicado a la supervisión periódica continua.*
- **Capacidad de personalización y puesta a punto.** *La organización debe aceptar la responsabilidad de personalizar y poner a punto la herramienta de SIEM implantada. Las implantaciones de SIEM listas para usar raramente tienen éxito o consiguen alcanzar todo el potencial que albergan.*

Revisemos los criterios más detenidamente.

En primer lugar, la empresa debe estar preparada para responder a las alertas poco después de que se produzcan. A pesar de que diversos proveedores suelen afirmar que “la empresa moderna trabaja en tiempo real y la seguridad debería hacerlo también”, según parece, en este momento hay pocas empresas que lo consigan. Antes de implantar una solución de SIEM, pregúntese en qué medida cuenta con una seguridad en tiempo real. Es posible que crea que en la mayoría de las ocasiones la seguridad es en tiempo real, o muy cercana a este. Los sistemas de detección de intrusiones en la red localizan ataques fuera de la conexión en cuestión de microsegundos, los cortafuegos bloquean las conexiones cuando estos se producen y la tecnología antivirus realiza el mayor esfuerzo posible para captar los virus en cuanto llegan.

Por tanto, pocas personas aceptan comprar un sistema de detección de intrusiones en la red (NIDS) que solo les notificará de un ataque después de que se hayan producido otros dos. Sin embargo, esas mismas personas tendrán a sus analistas de seguridad comprobando las alarmas de detección de intrusiones cada mañana. Si descubren un peligro grave, una respuesta en milisegundos del sistema NIDS carecerá importancia, pero la respuesta del personal cada hora sí la tendrá. Por tanto, la investigación de alertas a la mañana siguiente para descubrir un peligro grave para el sistema sigue siendo aceptable.

De manera semejante, si un archivo infectado por un virus llega y el software puede desinfectarlo en tiempo real, se resuelve el problema. Sin embargo, si el software antivirus detecta el código dañino pero no puede desinfectarlo automáticamente o ponerlo en cuarentena y, en su lugar, envía una alerta (lo que ocurre en el caso de algunas puertas traseras y troyanos), la tarea de responder vuelve a ser responsabilidad de los analistas que, muy probablemente, lleven varias horas de retraso. Dada la sofisticación de las amenazas actuales, con frecuencia este plazo es suficiente para que se produzca una vulneración grave, que podría llevar meses reparar. Como resultado, las reglas de alertas avanzadas y correlación con estados ofrecerán respuesta en menos de un segundo, pero usted debe estar preparado para responder a ellas.

Si una empresa no cuenta con un centro de operaciones de seguridad o prestaciones de supervisión, ya sea supervisión de seguridad u operativa, con acuerdos de nivel de servicio (SLA) rigurosos, muchas de las funciones de SIEM no se utilizarán a pleno rendimiento. Un primer paso habitual, a la hora de pasar del uso de los registros simplemente como respuesta hasta utilizarlos en una supervisión auténtica de la seguridad, es usar la supervisión periódica retrasada, que en realidad significa revisar los informes de registros por las mañanas. Esto puede lograrse con una herramienta de gestión de registros o de SIEM.

El criterio final del progreso está relacionado con la capacidad de puesta a punto y personalización. La empresa debe aceptar la responsabilidad de poner a punto y personalizar la herramienta de SIEM implantada para adaptar sus funciones avanzadas y personalizables al problema que la empresa debe hacer frente. Una segunda opción es contratar a una firma de consultoría que se encargue de realizar la puesta a punto. Cada empresa es única y, para que una solución de SIEM sea lo más eficaz posible, debe tener en cuenta los procesos empresariales únicos que existen. Esto podría implicar crear alertas, escribir reglas de correlación o personalizar los informes para obtener información sobre la postura de seguridad y conformidad de la empresa. Las implantaciones listas para usarse, con unas expectativas desmedidas, que consideran la solución de SIEM como una especie de “analista empaquetado”, raramente funcionan.

Si una empresa no cuenta con un centro de operaciones de seguridad o prestaciones de supervisión, ya sea supervisión de seguridad u operativa, con acuerdos de nivel de servicio (SLA) rigurosos, muchas de las funciones de SIEM no se utilizarán a pleno rendimiento.

El recorrido de una curva de madurez parte de la total ignorancia de los registros, pasando por la recopilación y retención de registros, la investigación ocasional y la revisión de registros periódica, hasta alcanzar la supervisión de la seguridad en tiempo casi real.

Las empresas que no tienen planes inmediatos para migrar desde, pongamos por caso, una solución de gestión de registros centrada en la conformidad deberían no obstante elegir una herramienta de registros que les permita pasar más adelante a una tecnología de SIEM. Incluso cuando no existen planes iniciales para ir más allá de la conformidad, muchas implantaciones de SIEM y de gestión de registros siguen los denominados modelos de conformidad plus, en los que la herramienta se adquiere para un marco normativo en particular, pero se utiliza en relación con muchos otros desafíos de seguridad y TI.

Tenga en cuenta que algunas herramientas de gestión de registros no ofrecen tal ruta de actualización a una solución de SIEM. Las herramientas más simples en particular, que solo permiten recopilar registros en bruto y realizar búsquedas en estos, pueden ser de gran utilidad, pero podrían no ofrecer un medio sencillo de lograr la normalización completa, la clasificación y otras mejoras de los datos de registros centradas en la seguridad. En general, si la herramienta recopila y retiene informes de registros en bruto y no se puede emparejar con una solución de SIEM que permita utilizar dichos datos para la supervisión y el análisis de la seguridad, no será posible avanzar hasta la supervisión. Cuando su empresa esté preparada para la supervisión en tiempo real, necesitará adquirir otras herramientas.

Dado que utilizar una solución de SIEM de modo eficaz le proporciona ventajas directas en lo que respecta a la reducción de las amenazas a través de análisis avanzados centrados en la seguridad (pero solo si su empresa está preparada para la tecnología de SIEM), el modelo de conformidad plus tiene sentido. En general, permite a la empresa acercarse más al ideal de la vista unificada en gestión de la seguridad.

Tras la tecnología de gestión de registros y SIEM: la curva de madurez

¿Qué ocurre después de que se implanten y se encuentren operativas soluciones de gestión de registros y de SIEM para ayudar con la conformidad y proporcionar ventajas de seguridad a una empresa? El recorrido de una curva de madurez parte de la total ignorancia de los registros, pasando por la recopilación y retención de registros, la investigación ocasional y la revisión de registros periódica, hasta alcanzar la supervisión de la seguridad en tiempo casi real.

La tendencia, en este caso, es pasar gradualmente de una posición de ignorancia a otra de reacción lenta y, a continuación, de reacción rápida hasta alcanzar, finalmente, una posición proactiva y consciente de lo que ocurre en todo su entorno de TI. Intentar pasar de una situación de ignorancia a otra proactiva raramente funciona, si es que llega a funcionar en algún caso.

fig. 5

Las empresas deberían mejorar continuamente la profundidad y el alcance de su implantación de SIEM mediante su integración con más sistemas, con el fin de hacer un uso más eficaz de las prestaciones analíticas de la solución de SIEM.

Superado este punto, ¿cuál es el siguiente paso de desarrollo? Para empezar, las empresas deberían mejorar continuamente la profundidad y el alcance de su implantación de SIEM mediante su integración con más sistemas, con el fin de hacer un uso más eficaz de las prestaciones analíticas de SIEM. Esto llega al núcleo de la misión de la tecnología de SIEM, la supervisión de la seguridad, y resuelve problemas nuevos, como el fraude, las amenazas internas, la supervisión de aplicaciones y la supervisión general de la actividad de los usuarios. La herramienta de SIEM empieza a adquirir más información y a ascender desde el nivel de la red hasta el de la aplicación, desde un número limitado de fuentes de datos hasta la distribución de toda la empresa. Al mismo tiempo, crece una organización de seguridad y, con ella, se desarrollan mejores procedimientos operativos aportan más agilidad a la empresa. Mientras amplía su implantación, es crucial que tenga presente que la estrategia por fases es la única forma de conseguir tener éxito.

¿Cuáles son algunos de los sistemas que mejorarían la misión de la tecnología de SIEM y le permitirían resolver otros problemas? Uno de los ejemplos más interesantes implica el uso de la información de los sistemas de gestión de identidades, como NetIQ Identity Manager. La información disponible en este sistema incluye la identidad del usuario, como el nombre real, la función profesional o la afiliación a unidad empresarial, junto con los derechos de acceso en varios sistemas y aplicaciones. Saber quién es el usuario y qué tipo de autorizaciones tiene es indispensable para supervisar la actividad interna. Por ejemplo, le permite crear una identidad unificada para cada usuario y, a continuación, utilizar dicha identidad para supervisar las acciones del usuario en varios sistemas, incluso con nombres de usuario y cuentas diferentes.

Es importante ser consciente de que, aunque muchos proveedores afirman ofrecer integración de la identidad, la mayoría ejecuta solo una sencilla búsqueda de protocolo ligero de acceso a directorios (LDAP). Estos sistemas no aprovechan todos los datos avanzados que puede proporcionar un sistema de identidad para ayudar a un producto de SIEM a determinar si las actividades son dañinas o importantes desde el punto de vista normativo.

Además, la integración del gestor de identidades permite que un producto de SIEM diferencie los inicios de sesión oficiales, autorizados, de los intentos de inicio de sesión de puerta trasera, no autorizados. Dicha integración permite, asimismo, automatizar la supervisión de la separación de tareas (SoD), al hacer que la solución de SIEM reconozca aquellas funciones que no tienen autorización para llevar a cabo acciones específicas.

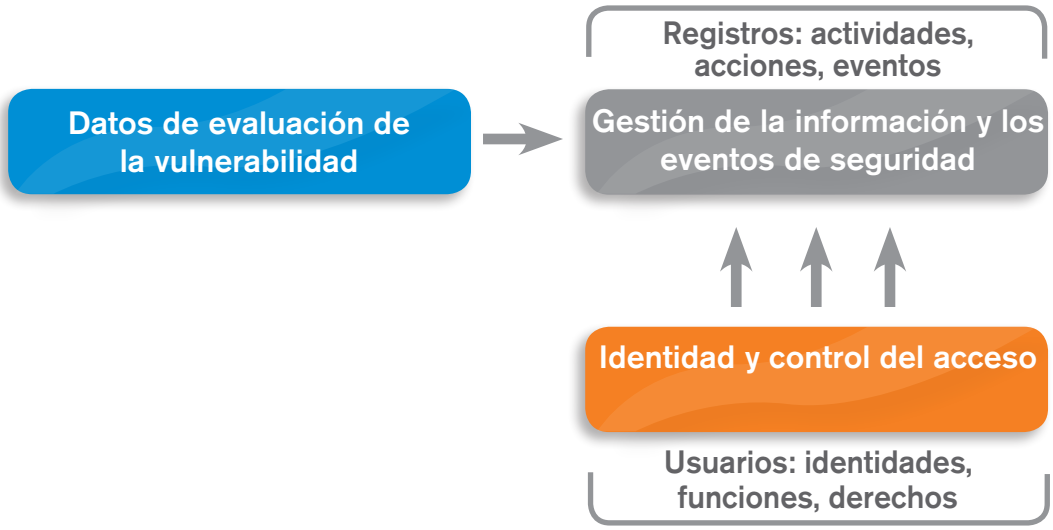

fig. 6

Además, un sistema de gestión de activos incluirá información detallada similar en todos los recursos de TI dentro de la empresa. Igual que en el caso de los usuarios, podemos extraer las funciones empresariales de los activos, el nivel de importancia empresarial, la relevancia para la conformidad, los nombres y ubicaciones de administrador, así como otro tipo de información sobre qué función ejecutan los activos y quién es responsable de estos. Tal información mejora radicalmente las funciones de cálculo de riesgos y establecimiento de prioridades de eventos de la solución de SIEM. Es importante ser consciente de que, aunque muchos proveedores afirman ofrecer integración de la identidad, la mayoría ejecuta solo una sencilla búsqueda de Protocolo ligero de acceso a directorios (LDAP). Estos sistemas no aprovechan todos los datos avanzados que puede proporcionar un sistema de identidad para ayudar a un producto de SIEM a determinar si las actividades son dañinas o importantes desde el punto de vista normativo.

Es posible lograr niveles superiores de integración y, por tanto, mayor conocimiento, mediante la integración del producto SIEM con bases de datos de gestión de configuraciones (CMDB). Tales integraciones permiten a un producto de SIEM correlacionar los cambios detectados en los sistemas y aplicaciones con los cambios aprobados y autorizados.

Errores

Al planificar e implantar una infraestructura de recopilación y análisis de registros, ya sea para una solución de SIEM o de gestión de registros, las empresas a menudo descubren que no están desarrollando todo el potencial de dichos sistemas. De hecho, a veces notan una pérdida de eficacia. Esto suele deberse a los siguientes errores habituales de implantación.

Carecer de registro, aunque es el error más obvio, se produce con demasiado frecuencia, incluso en la época actual de normativas como Sarbanes-Oxley (SOX) y PCI-DSS. Este error destruye cualquier oportunidad de beneficiarse de la tecnología de gestión de registros o de SIEM.

Otra versión del mismo error es carecer de registro y no ser consciente de ello hasta que ya es demasiado tarde.

¿En qué sentido puede ser demasiado tarde? No disponer de registros puede conducir a la pérdida de ingresos. Los requisitos de registro de la norma PCI-DSS implican que las infracciones pueden derivar en la cancelación de sus privilegios de procesamiento de tarjetas de crédito por parte de Visa o MasterCard, lo que le apartaría del negocio (daño a la reputación). Imagine, por ejemplo, que se han sustraído algunos números de tarjetas de crédito de su base de datos, pero los medios han informado de un robo de 40 millones de tarjetas de crédito y usted no ha podido demostrar lo contrario (e incluso su inocencia). No hay más que ver en los medios los diversos escándalos relacionados con SOX.

Cuando se han puesto en funcionamiento tanto la herramienta de SIEM como la de gestión de registros, su empresa puede avanzar en el proceso de maduración hacia una visibilidad completa de la red y las aplicaciones, la supervisión de la actividad de los usuarios y la integración con distintos sistemas.

Incluso las empresas bien preparadas caen en este error. Considere este ejemplo reciente. ¿Tiene su servidor Web registros activados? Claro, se trata de una opción predeterminada en los dos servidores Web más populares: Apache y Microsoft IIS. ¿Tiene el sistema operativo de su servidor mensajes de registro? Claro, nadie ha cancelado */var/log/messages*.

Los requisitos de registro de la norma PCI-DSS implican que las infracciones pueden derivar en la cancelación de sus privilegios de procesamiento de tarjetas de crédito por parte de Visa o MasterCard, lo que le apartaría del negocio.

El objetivo es saber lo que está pasando en su entorno y poder ofrecerle una respuesta, así como predecir lo que va a ocurrir más adelante.

Pero, ¿y su base de datos*?* La opción predeterminada de Oracle es no ejecutar ningún registro de auditoría del acceso a datos. Y Microsoft SQL, ¿sale mejor parado? Desgraciadamente, la respuesta es no. Es necesario profundizar en el sistema para empezar incluso un nivel moderado de generación de seguimiento de auditoría.

Por tanto, evitar este error suele requerir el ir más allá de los valores predeterminados y asegurarse de que el software y el hardware tienen cierto nivel de registro activado. En el caso de Oracle, por ejemplo, podría reducirse a garantizar que la variable de seguimiento de auditoría se configura en "db". Sin embargo, es posible que entrañe mayores complicaciones en el caso de otros sistemas.

No revisar los registros **es el segundo error.** Aunque asegurarse de que se producen, recopilan y almacenan los registros es importante, es solo el medio para alcanzar un fin. El objetivo es saber lo que está pasando en su entorno y poder ofrecerle una respuesta, así como predecir lo que va a ocurrir más adelante. Según hemos descrito anteriormente, se trata de una etapa, no del destino final. Si su empresa ha pasado de ignorar los registros a recopilarlos, es importante tener en cuenta que, en última instancia, tendrá que revisarlos. Si recopila registros y no los revisa, solo está documentando su propia negligencia, sobre todo si su directiva de seguridad de TI estipula la revisión de registros.

Por tanto, una vez que cuenta con la tecnología necesaria y se recopilan los registros, debe disponer de un proceso para la supervisión continua y comprobar que se conecte con las acciones y derivaciones posibles, cuando corresponda. Asimismo, el personal que revisa y supervisa los registros debe contar con información suficiente para determinar qué significan realmente y qué medidas deben tomarse, si fuera necesario.

Tenga en cuenta que algunas empresas dan un pequeño paso en la dirección adecuada: revisan los registros tras una incidencia importante, como un peligro, fuga de información o fallo misterioso del servidor, y evitan llevar a cabo la supervisión continua y revisión de registros, normalmente utilizando la excusa habitual de la falta de recursos. Esto les proporciona la ventaja de la reacción gracias al análisis de registros y, aunque esto es importante, no llegan a beneficiarse de la estrategia proactiva, es decir, saber cuándo están a punto de producirse problemas o cuándo van a empeorar. Si revisa los registros, por ejemplo, podría darse cuenta de que el failover fue activado por un cortafuegos, y que, aunque la conexión siguió funcionando, sin duda vale la pena examinar el incidente. Si no lo hace y pierde la conexión de su red, tendrá que confiar en sus siempre útiles registros para investigar por qué fallaron ambos dispositivos de failover.

Es igualmente esencial resaltar que ciertos tipos de empresa tienen que comprobar los archivos de registros y los seguimientos de auditorías como consecuencia de algún tipo de presión normativa**.** Como mencionamos previamente, la normativa HIPAA obliga a las empresas médicas a establecer un programa de informe y análisis de auditoría. La norma de seguridad de los datos PCI-DSS incluye disposiciones tanto para la recopilación de registros como para su revisión periódica, lo que pone de relieve que la recopilación de registros no sirve por sí sola.

A menudo, sobre todo en el caso de los ataques de origen interno, las incidencias se descubren mucho después de que se cometiera el delito o uso indebido, a veces incluso varios meses más tarde.

El tercer error común es almacenar los registros durante un periodo demasiado breve. Es posible que el almacén de registros operativo de un sistema de SIEM retenga los eventos normalizados durante 30 días, pero para una retención a largo plazo se requiere un sistema de gestión de registros. Esto hace creer al equipo de seguridad o de operaciones de TI que cuenta con todos los registros necesarios para la supervisión e investigación, o la resolución de problemas, hasta que se produce una incidencia y descubre con horror que todos los registros han desaparecido como consecuencia de una política de retención poco previsora. A menudo, sobre todo en el caso de los ataques de origen interno, las incidencias se descubren mucho después de que se cometiera el delito o uso indebido, a veces incluso varios meses más tarde. Puede que consiga algún ahorro en hardware de almacenamiento, pero arriesga perder diez veces más como resultado de sanciones normativas.

Si la reducción del gasto es un factor fundamental, la solución puede ser dividir la retención en dos partes: almacenamiento en línea a corto plazo, que es más caro, y almacenamiento fuera de línea a largo plazo, que resulta bastante más económico. Una buena herramienta de gestión de registros le permitirá buscar a través de ambos almacenes de forma transparente, sin necesidad de trasladar datos. Es también frecuente una estrategia más eficaz en tres niveles que supera algunas de las limitaciones del anterior. En este caso, un almacenamiento en línea a corto plazo se complementa con otro casi en línea que permite seguir accediendo a los registros y realizando búsquedas. Los informes de registros más antiguos y menos relevantes se descargan en el tercer nivel, como una cinta o DVD, donde se pueden guardar sin gran gasto. Sin embargo, no hay modo de acceder de forma selectiva a los registros necesarios. Por citar un ejemplo, una institución financiera almacenaba los registros en línea durante 90 días; a continuación, en almacenamiento casi en línea con capacidad de búsqueda del sistema de gestión de registros durante dos años; y, finalmente, en cinta durante siete años, o incluso más en algunos casos.

El cuarto error está relacionado con el establecimiento de prioridades de los informes de registros. Aunque sea necesario cierto sentido de la prioridad para organizar mejor las tareas de análisis de registros, el error habitual en la actualidad es establecer la prioridad de los informes de registros antes de recopilarlos. De hecho, algunos documentos de mejores prácticas recomiendan incluso recopilar solo “los datos importantes”. Sin embargo, ¿qué es importante? En este punto es donde los documentos de guía mencionados cojean, ya que no lo especifican de un modo realmente útil. Aunque existen diversas estrategias en relación con este problema, pueden conducir a fisuras mayúsculas en la postura de seguridad e incluso socavar sus esfuerzos de conformidad con la normativa.

Debe asegurarse de que los registros de aplicaciones se recopilan y están disponibles para su análisis, así como para la retención a largo plazo. Esto puede lograrse configurando su software de gestión de registros para que los recopile y estableciendo una directiva de revisión de registros. Ambas medidas se deben aplicar a la revisión basada en incidencias y a la revisión de registros periódica proactiva.

Por ejemplo, muchas personas afirmarán que los registros de detección y prevención de intrusiones en la red son, por naturaleza, más importantes que, pongamos por caso, los registros del concentrador de red privada virtual (VPN). Puede que esto sea verdad en un mundo en el que dominan completamente las amenazas externas y todos los empleados y socios son dignos de confianza. Si tiene que llevar a cabo una investigación interna sobre una fuga de datos o una infección con software dañino, lo más probable es que necesite los registros de VPN, junto con los de servidores y estaciones de trabajo. De este modo, se puede defender igualmente la enorme importancia de cualquier otro tipo de registro, lo que revelaría la necesidad de recopilar todos, o la mayoría, de los informes de registros producidos. Pero, ¿es posible hacerlo? Antes de contestar a esta pregunta, intente responder si es posible tomar la decisión adecuada sobre qué registros son más importantes antes incluso de verlos, y dejará de parecerle un problema sin solución. De hecho, existen soluciones rentables que permiten lograrlo.

El modo de evitar este error es implantar una solución de gestión de registros antes que una de SIEM, como indicamos anteriormente. Esto garantizará que todos los registros necesarios están disponibles para el análisis, incluso cuando un motor de correlación de SIEM solo llegue a ver una porción de estos.

El último error consiste en ignorar los registros de las aplicaciones al centrarse exclusivamente en los dispositivos del perímetro y la red interna y, quizás, los servidores, pero no llegar a un nivel superior para comprobar el registro de aplicaciones.

El ámbito de las aplicaciones empresariales abarca desde las aplicaciones SAP y PeopleSoft, hasta aplicaciones pequeñas de desarrollo interno que, no obstante, gestionan procesos de misión crítica en numerosas empresas. También existen aplicaciones legadas que se ejecutan en sistemas mainframe y de categoría media y, con frecuencia, llevan a cabo los procesos empresariales esenciales. La disponibilidad y calidad de los registros difieren enormemente en las aplicaciones: desde ser inexistentes (el caso de muchas aplicaciones desarrolladas internamente) hasta extremadamente detallados y abundantes (el caso de muchas aplicaciones de mainframe). La falta de estándares de registro comunes, e incluso de orientación sobre el registro, para los desarrolladores de software hace que los registros de aplicaciones planteen numerosos retos. Afortunadamente, los esfuerzos futuros, como el Common Event Expression (CEE) de MITRE, vendrán a poner remedio a este problema.

A pesar de los desafíos, debe asegurarse de que los registros de aplicaciones se recopilan y están disponibles para su análisis, así como para la retención a largo plazo. Esto puede lograrse configurando su software de gestión de registros para que los recopile y estableciendo una directiva de revisión de registros. Ambas medidas se deben aplicar a la revisión basada en incidencias y a la revisión de registros periódica proactiva. Busque proveedores que facilitan la configuración de sus sistemas para que recopilen registros de las aplicaciones personalizadas, ya que estas suelen ser las más importantes. Después, puede configurar el producto de SIEM para analizar los registros con fines de seguridad, junto con los registros de red, entre otros.

Conclusiones

Una de las principales conclusiones del presente trabajo es la necesidad de recordar que todo el mundo tiene registros y que esto significa, en última instancia, que todo el mundo necesita gestionar los registros. En su sentido más amplio, gestión de registros significa simplemente ocuparse de los registros. Y si usted tiene registros, tiene que ocuparse de ellos, aunque solo sea porque numerosas normativas lo exigen.

Asimismo, es importante recordar que los registros se utilizan para un gran número de situaciones, desde la tradicional respuesta a incidencias hasta otras extremadamente esotéricas. La mayoría de usos de los registros tienen lugar mucho después de que el evento se haya producido y haya quedado recogido en los registros. Es mucho más sencillo estar preparado para responder que para supervisar.

Es posible que su empresa necesite volver a la "escuela" del registro antes de obtener la "licenciatura" en SIEM. Tal progreso requiere la habilidad de responder a las alertas, así como de personalizar y poner a punto los productos.

Poner en funcionamiento tanto la herramienta de SIEM como la de gestión de registros permitirá a su empresa avanzar en el proceso de maduración hasta una visibilidad completa de la red y las aplicaciones, la supervisión de la actividad de los usuarios y la integración con distintos sistemas.

Es posible que su empresa necesite volver a la "escuela" del registro antes de obtener la "licenciatura" en SIEM. Tal progreso requiere la habilidad de responder a las alertas, así como de personalizar y poner a punto los productos.

Acerca del autor

El Dr. Anton Chuvakin (**http://www.chuvakin.org**) es un conocido experto en seguridad, especializado en el campo de la gestión de registros y la conformidad con la norma PCI-DSS. Es autor de dos libros, "Security Warrior" (El guerrero de la seguridad) y "PCI Compliance" (Conformidad de PCI), y colaborador en "Know Your Enemy II" (Conoce a tu enemigo II) e "Information Security Management Handbook" (Manual de gestión de seguridad de la información), entre otros. Anton ha publicado decenas de artículos sobre gestión de registros, correlación, análisis de datos, PCI-DSS y gestión de la seguridad (para ver una lista, visite **www.info-secure.org**). Su blog, **www.securitywarrior.org** es uno de los más populares en el sector. Además, Anton imparte clases y realiza presentaciones en numerosas conferencias de seguridad en todo el mundo. Recientemente se ha dirigido a audiencias de Estados Unidos, Reino Unido, Singapur, España y Rusia, entre otros países. Asimismo, trabaja en las normas de seguridad emergentes y colabora en las juntas asesoras de varias iniciativas de seguridad.

Los clientes y socios eligen NetIQ para afrontar de manera rentable los retos que plantean la protección de la información y la complejidad de las operaciones de TI.

En la actualidad, se encuentra desarrollando su práctica de consultoría, **www.securitywarriorconsulting.com**, enfocada al registro y la conformidad con la norma PCI-DSS para proveedores de seguridad y empresas de la lista Fortune 500. El Dr. Anton Chuvakin fue director de Soluciones de conformidad de PCI en Qualys en el pasado. Anteriormente, había trabajado en Log Logic como experto jefe de registro, y sus responsabilidades incluían la oferta de formación global sobre la importancia de los registros para la seguridad, la conformidad y las operaciones. Antes, Anton estuvo empleado como proveedor de seguridad en un puesto de gestión estratégica de productos. Anton es doctor por la Stony Brook University.

Acerca de NetIQ

NetIQ es una compañía de software empresarial con un enfoque intensivo en el éxito del cliente. Los clientes y socios eligen NetIQ para afrontar de manera rentable los retos que plantean la protección de la información y la complejidad de las operaciones de TI. Nuestra cartera de soluciones ampliables y automatizadas para la gestión de la seguridad y el cumplimiento de las regulaciones, la identidad y el acceso, y el rendimiento y la disponibilidad, junto con nuestro enfoque práctico y centrado en la solución de retos de TI, ayuda a los clientes a lograr un mayor valor estratégico, una mejora demostrable de la actividad empresarial y un gran ahorro, en comparación con otras opciones alternativas.

Para obtener más información, visite: **www.netiq.com**

NetIQ
Argentina
+54 11 5258 8899

Chile
+56 2 2864 5629

Colombia
+57 1 622 2766

México
+52 55 5284 2700

Panamá
+507 2 039291

España
+34 91 781 5004

Venezuela
+58 212 267 6568

contact-es@netiq.com
www.netiq.com/communities
www.netiq.com

Para obtener una lista completa de nuestras oficinas en América del Norte, Europa, Oriente Medio, África, Asia-Pacífico y América Latina, visite www.netiq.com/contacts.

www.netiq.com

www.netiq.com